

From: traceback-notice@tracebacks.org

To: jrolivarm@gmail.com, noc@smartbiztel.com

Date: 26 Jun 20 17:44 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

By way of introduction, my name is Patrick Halley, and I coordinate the efforts of USTelecom's Industry Traceback Group (ITG). We are writing to request your assistance on industry efforts to protect consumers from fraudulent, abusive or potentially unlawful robocalls. My contact information is listed below, and I would be more than happy to discuss this request with you over the phone.

A member of USTelecom's ITG recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin (call details with date(s) are listed below). We request that you assist industry stakeholders who are engaging in traceback efforts in order to help identify the source of this potentially fraudulent, abusive or unlawful network traffic. To assist us in our efforts, **we are asking that you respond to this traceback inquiry as soon as possible, but no later than three business days from now.**

USTelecom, a 501(c)(6) trade association, represents service providers and suppliers for the telecommunications industry and leads the ITG, a collaborative effort of companies from across the wireline, wireless, VoIP and cable industries that actively trace and identify the source of illegal robocalls. The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information of about the ITG or a list of the current members, see USTelecom's [website](#).

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." In addition, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

The Federal Communications Commission's (FCC) Enforcement Bureau has sent letters to carriers that have been non-responsive to ITG traceback requests. The letters "urge" carriers to "to cooperate with the USTelecom Industry Traceback Group's program aimed at identifying the source of illegal robocalls and harmful spoofed calls." The ITG has received recognition at all levels of government, including the FCC, the Federal Trade Commission (FTC) and all 50 State Attorneys General.

We are asking that you submit your response to this inquiry via our secure on-line portal, where you can see additional detail about all traceback requests involving your network. With respect to the call details below, please provide us with the following:

1. Please investigate the source of this traffic and respond with the identity of the upstream carrier(s) that sent the traffic into your network, or if one of your end users originated the traffic, please identify that end user. **We ask that you use the link below to access the portal and use the drop-down selector to provide this information.**
2. If, in investigating this traffic, the end user(s) originating the traffic are able to demonstrate to you that the traffic complies with applicable United States laws and regulations, please respond via email to me with the description of the traffic, the identity of the customer, and the customer's explanation.
3. As you investigate this matter, please take appropriate action on your network to ensure compliance with applicable United States laws and regulations, and inform me of the action you have taken.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream carriers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call 202-756-6999 or contact me via reply email should you have any questions, or would like to discuss.

Best Regards,

Patrick Halley
Senior Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
<https://traceback.ustelecom.org/Form/Login/r;REDACTED?t=rqfexUkqd>
(URL is a private login; do not share.)

Call Details for Incident #2640 (new)

Date/Time: 2020-06-26 15:34:00 UTC

To: +14072223658

From: +14072613544

Campaign: Utility-30MinDisconnect

Likely FRAUD. Recorded message says your electric service will be disconnected in 30 minutes; press 1 to make payment arrangements. Utility company is not identified. Assorted toll-free numbers used as caller-ID.

From: traceback-notice@tracebacks.org

To: jrolivarm@gmail.com, noc@smartbiztel.com

Date: 30 Jun 20 07:38 UTC

USTELECOM

THE BROADBAND ASSOCIATION

This is a reminder regarding a recent request we sent for call detail information from the USTelecom Industry Traceback Group regarding a suspected illegal robocall.

Please use the link below to access the Traceback Secure Web Portal and fill in the requested information regarding the source of the call(s).

We would appreciate a response as quickly as possible; ideally in 4 hours or less and no longer than one business day.

For help or questions, email traceback-notice@ustelecom.org or call 202-756-6999.

Submit your response via our secure on-line portal:

<https://traceback.ustelecom.org/Form/Login/r;REDACTED?t=rBDBBqmn3z>

(URL is a private login; do not share.)

Call Details for Incident #2640 (3d13h ago)

Date/Time: 2020-06-26 15:34:00 UTC

To: +14072223658

From: +14072613544

Campaign: Utility-30MinDisconnect

Likely FRAUD. Recorded message says your electric service will be disconnected in 30 minutes; press 1 to make payment arrangements. Utility company is not identified. Assorted toll-free numbers used as caller-ID.

From: traceback-notice@tracebacks.org

To: jrolivarm@gmail.com, noc@smartbiztel.com

Date: 30 Jun 20 19:42 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

By way of introduction, my name is Patrick Halley, and I coordinate the efforts of USTelecom's Industry Traceback Group (ITG). We are writing to request your assistance on industry efforts to protect consumers from fraudulent, abusive or potentially unlawful robocalls. My contact information is listed below, and I would be more than happy to discuss this request with you over the phone.

A member of USTelecom's ITG recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin (call details with date(s) are listed below). We request that you assist industry stakeholders who are engaging in traceback efforts in order to help identify the source of this potentially fraudulent, abusive or unlawful network traffic. To assist us in our efforts, **we are asking that you respond to this traceback inquiry as soon as possible, but no later than three business days from now.**

USTelecom, a 501(c)(6) trade association, represents service providers and suppliers for the telecommunications industry and leads the ITG, a collaborative effort of companies from across the wireline, wireless, VoIP and cable industries that actively trace and identify the source of illegal robocalls. The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information of about the ITG or a list of the current members, see USTelecom's [website](#).

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." In addition, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

The Federal Communications Commission's (FCC) Enforcement Bureau has sent letters to carriers that have been non-responsive to ITG traceback requests. The letters "urge" carriers to "to cooperate with the USTelecom Industry Traceback Group's program aimed at identifying the source of illegal robocalls and harmful spoofed calls." The ITG has received recognition at all levels of government, including the FCC, the Federal Trade Commission (FTC) and all 50 State Attorneys General.

We are asking that you submit your response to this inquiry via our secure on-line portal, where you can see additional detail about all traceback requests involving your network. With respect to the call details below, please provide us with the following:

1. Please investigate the source of this traffic and respond with the identity of the upstream carrier(s) that sent the traffic into your network, or if one of your end users originated the traffic, please identify that end user. **We ask that you use the link below to access the portal and use the drop-down selector to provide this information.**
2. If, in investigating this traffic, the end user(s) originating the traffic are able to demonstrate to you that the traffic complies with applicable United States laws and regulations, please respond via email to me with the description of the traffic, the identity of the customer, and the customer's explanation.
3. As you investigate this matter, please take appropriate action on your network to ensure compliance with applicable United States laws and regulations, and inform me of the action you have taken.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream carriers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call 202-756-6999 or contact me via reply email should you have any questions, or would like to discuss.

Best Regards,

Patrick Halley
Senior Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
<https://traceback.ustelecom.org/Form/Login/r;REDACTED?t=tnhYXDv>
(URL is a private login; do not share.)

Call Details for Incident #2659 (new)

Date/Time: 2020-06-30 16:41:00 UTC

To: +14053030584

From: +12109421156

Campaign: SSA-P1-BenefitsCanceled (GImpS)

Captured recordings suggest these calls are perpetrating a SERIOUS FRAUD. Caller is impersonating a federal official. Automated message threatens that social security benefits will be canceled. Caller-ID appears to be a random toll-free number. Called party is asked to press 1 to speak to an agent. Caller-ID is random (different on each call) so blocking the ANI is not effective. This call is just one example representative of millions of similar calls. Originators please search your records for similar traffic.

From: traceback-notice@tracebacks.org

To: jrolivarm@gmail.com, noc@smartbiztel.com

Date: 30 Jun 20 20:07 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

By way of introduction, my name is Patrick Halley, and I coordinate the efforts of USTelecom's Industry Traceback Group (ITG). We are writing to request your assistance on industry efforts to protect consumers from fraudulent, abusive or potentially unlawful robocalls. My contact information is listed below, and I would be more than happy to discuss this request with you over the phone.

A member of USTelecom's ITG recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin (call details with date(s) are listed below). We request that you assist industry stakeholders who are engaging in traceback efforts in order to help identify the source of this potentially fraudulent, abusive or unlawful network traffic. To assist us in our efforts, **we are asking that you respond to this traceback inquiry as soon as possible, but no later than three business days from now.**

USTelecom, a 501(c)(6) trade association, represents service providers and suppliers for the telecommunications industry and leads the ITG, a collaborative effort of companies from across the wireline, wireless, VoIP and cable industries that actively trace and identify the source of illegal robocalls. The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information of about the ITG or a list of the current members, see USTelecom's [website](#).

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." In addition, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

The Federal Communications Commission's (FCC) Enforcement Bureau has sent letters to carriers that have been non-responsive to ITG traceback requests. The letters "urge" carriers to "to cooperate with the USTelecom Industry Traceback Group's program aimed at identifying the source of illegal robocalls and harmful spoofed calls." The ITG has received recognition at all levels of government, including the FCC, the Federal Trade Commission (FTC) and all 50 State Attorneys General.

We are asking that you submit your response to this inquiry via our secure on-line portal, where you can see additional detail about all traceback requests involving your network. With respect to the call details below, please provide us with the following:

1. Please investigate the source of this traffic and respond with the identity of the upstream carrier(s) that sent the traffic into your network, or if one of your end users originated the traffic, please identify that end user. **We ask that you use the link below to access the portal and use the drop-down selector to provide this information.**
2. If, in investigating this traffic, the end user(s) originating the traffic are able to demonstrate to you that the traffic complies with applicable United States laws and regulations, please respond via email to me with the description of the traffic, the identity of the customer, and the customer's explanation.
3. As you investigate this matter, please take appropriate action on your network to ensure compliance with applicable United States laws and regulations, and inform me of the action you have taken.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream carriers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call 202-756-6999 or contact me via reply email should you have any questions, or would like to discuss.

Best Regards,

Patrick Halley
Senior Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
<https://traceback.ustelecom.org/Form/Login/r:REDACTED?t=WV7MYO4Jf>
(URL is a private login; do not share.)

Call Details for Incident #2644 (new)

Date/Time: 2020-06-26 14:32:00 UTC
To: +15016818212
From: +15016815568
Campaign: USTreas-EnforcementAction-GImp
FRAUD. Claims to be from US Treasury regarding an enforcement action. Impersonates a government official. Recorded/automated voice to wireless numbers generally prohibited. Random spoofing of Caller-ID. Blocking the ANI is not effective.

Call Details for Incident #2659 (25m ago)

Date/Time: 2020-06-30 16:41:00 UTC
To: +14053030584
From: +12109421156
Campaign: SSA-P1-BenefitsCanceled (GImpS)
Captured recordings suggest these calls are perpetrating a SERIOUS FRAUD. Caller is impersonating a federal official. Automated message threatens that social security benefits will be canceled. Caller-ID appears to be a random toll-free number. Called party is asked to press 1 to speak to an agent. Caller-ID is random (different on each call) so blocking the ANI is not effective. This call is just one example representative of millions of similar calls. Originators please search your records for similar traffic.

From: traceback-notice@tracebacks.org

To: jrolivarm@gmail.com, noc@smartbiztel.com

Date: 08 Jul 20 20:01 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

By way of introduction, my name is Patrick Halley, and I coordinate the efforts of USTelecom's Industry Traceback Group (ITG). We are writing to request your assistance on industry efforts to protect consumers from fraudulent, abusive or potentially unlawful robocalls. My contact information is listed below, and I would be more than happy to discuss this request with you over the phone.

A member of USTelecom's ITG recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin (call details with date(s) are listed below). We request that you assist industry stakeholders who are engaging in traceback efforts in order to help identify the source of this potentially fraudulent, abusive or unlawful network traffic. To assist us in our efforts, **we are asking that you respond to this traceback inquiry as soon as possible, but no later than three business days from now.**

USTelecom, a 501(c)(6) trade association, represents service providers and suppliers for the telecommunications industry and leads the ITG, a collaborative effort of companies from across the wireline, wireless, VoIP and cable industries that actively trace and identify the source of illegal robocalls. The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information of about the ITG or a list of the current members, see USTelecom's [website](#).

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." In addition, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

The Federal Communications Commission's (FCC) Enforcement Bureau has sent letters to carriers that have been non-responsive to ITG traceback requests. The letters "urge" carriers to "to cooperate with the USTelecom Industry Traceback Group's program aimed at identifying the source of illegal robocalls and harmful spoofed calls." The ITG has received recognition at all levels of government, including the FCC, the Federal Trade Commission (FTC) and all 50 State Attorneys General.

We are asking that you submit your response to this inquiry via our secure on-line portal, where you can see additional detail about all traceback requests involving your network. With respect to the call details below, please provide us with the following:

1. Please investigate the source of this traffic and respond with the identity of the upstream carrier(s) that sent the traffic into your network, or if one of your end users originated the traffic, please identify that end user. **We ask that you use the link below to access the portal and use the drop-down selector to provide this information.**
2. If, in investigating this traffic, the end user(s) originating the traffic are able to demonstrate to you that the traffic complies with applicable United States laws and regulations, please respond via email to me with the description of the traffic, the identity of the customer, and the customer's explanation.
3. As you investigate this matter, please take appropriate action on your network to ensure compliance with applicable United States laws and regulations, and inform me of the action you have taken.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream carriers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call 202-756-6999 or contact me via reply email should you have any questions, or would like to discuss.

Best Regards,

Patrick Halley
Senior Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
<https://traceback.ustelecom.org/Form/Login/r;REDACTED?t=ITKGaNbmTW>
(URL is a private login; do not share.)

Call Details for Incident #2708 (new)

Date/Time: 2020-07-08 15:46:00 UTC

To: +15756492707

From: +19152453792

Campaign: Utility-30MinDisconnect

Likely FRAUD. Recorded message says your electric service will be disconnected in 30 minutes; press 1 to make payment arrangements. Utility company is not identified. Assorted toll-free numbers used as caller-ID.

From: traceback-notice@tracebacks.org

To: jrolivarm@gmail.com, noc@smartbiztel.com

Date: 08 Jul 20 20:07 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

By way of introduction, my name is Patrick Halley, and I coordinate the efforts of USTelecom's Industry Traceback Group (ITG). We are writing to request your assistance on industry efforts to protect consumers from fraudulent, abusive or potentially unlawful robocalls. My contact information is listed below, and I would be more than happy to discuss this request with you over the phone.

A member of USTelecom's ITG recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin (call details with date(s) are listed below). We request that you assist industry stakeholders who are engaging in traceback efforts in order to help identify the source of this potentially fraudulent, abusive or unlawful network traffic. To assist us in our efforts, **we are asking that you respond to this traceback inquiry as soon as possible, but no later than three business days from now.**

USTelecom, a 501(c)(6) trade association, represents service providers and suppliers for the telecommunications industry and leads the ITG, a collaborative effort of companies from across the wireline, wireless, VoIP and cable industries that actively trace and identify the source of illegal robocalls. The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information of about the ITG or a list of the current members, see USTelecom's [website](#).

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." In addition, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

The Federal Communications Commission's (FCC) Enforcement Bureau has sent letters to carriers that have been non-responsive to ITG traceback requests. The letters "urge" carriers to "to cooperate with the USTelecom Industry Traceback Group's program aimed at identifying the source of illegal robocalls and harmful spoofed calls." The ITG has received recognition at all levels of government, including the FCC, the Federal Trade Commission (FTC) and all 50 State Attorneys General.

We are asking that you submit your response to this inquiry via our secure on-line portal, where you can see additional detail about all traceback requests involving your network. With respect to the call details below, please provide us with the following:

1. Please investigate the source of this traffic and respond with the identity of the upstream carrier(s) that sent the traffic into your network, or if one of your end users originated the traffic, please identify that end user. **We ask that you use the link below to access the portal and use the drop-down selector to provide this information.**
2. If, in investigating this traffic, the end user(s) originating the traffic are able to demonstrate to you that the traffic complies with applicable United States laws and regulations, please respond via email to me with the description of the traffic, the identity of the customer, and the customer's explanation.
3. As you investigate this matter, please take appropriate action on your network to ensure compliance with applicable United States laws and regulations, and inform me of the action you have taken.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream carriers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call 202-756-6999 or contact me via reply email should you have any questions, or would like to discuss.

Best Regards,

Patrick Halley
Senior Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
<https://traceback.ustelecom.org/Form/Login/r;REDACTED?t=anIIFN1K>
(URL is a private login; do not share.)

Call Details for Incident #2709 (new)

Date/Time:

2020-07-08 15:46:00 UTC

To:

+15752022683

From:

+19152453792

Campaign:

Utility-30MinDisconnect

Likely FRAUD. Recorded message says your electric service will be disconnected in 30 minutes; press 1 to make payment arrangements. Utility company is not identified. Assorted toll-free numbers used as caller-ID.

Call Details for Incident #2708 (6m ago)

Date/Time:

2020-07-08 15:46:00 UTC

To:

+15756492707

From:

+19152453792

Campaign:

Utility-30MinDisconnect

(see description above)

From: traceback-notice@tracebacks.org

To: jrolivarm@gmail.com, noc@smartbiztel.com

Date: 08 Jul 20 20:07 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

By way of introduction, my name is Patrick Halley, and I coordinate the efforts of USTelecom's Industry Traceback Group (ITG). We are writing to request your assistance on industry efforts to protect consumers from fraudulent, abusive or potentially unlawful robocalls. My contact information is listed below, and I would be more than happy to discuss this request with you over the phone.

A member of USTelecom's ITG recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin (call details with date(s) are listed below). We request that you assist industry stakeholders who are engaging in traceback efforts in order to help identify the source of this potentially fraudulent, abusive or unlawful network traffic. To assist us in our efforts, **we are asking that you respond to this traceback inquiry as soon as possible, but no later than three business days from now.**

USTelecom, a 501(c)(6) trade association, represents service providers and suppliers for the telecommunications industry and leads the ITG, a collaborative effort of companies from across the wireline, wireless, VoIP and cable industries that actively trace and identify the source of illegal robocalls. The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information of about the ITG or a list of the current members, see USTelecom's [website](#).

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." In addition, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

The Federal Communications Commission's (FCC) Enforcement Bureau has sent letters to carriers that have been non-responsive to ITG traceback requests. The letters "urge" carriers to "to cooperate with the USTelecom Industry Traceback Group's program aimed at identifying the source of illegal robocalls and harmful spoofed calls." The ITG has received recognition at all levels of government, including the FCC, the Federal Trade Commission (FTC) and all 50 State Attorneys General.

We are asking that you submit your response to this inquiry via our secure on-line portal, where you can see additional detail about all traceback requests involving your network. With respect to the call details below, please provide us with the following:

1. Please investigate the source of this traffic and respond with the identity of the upstream carrier(s) that sent the traffic into your network, or if one of your end users originated the traffic, please identify that end user. **We ask that you use the link below to access the portal and use the drop-down selector to provide this information.**
2. If, in investigating this traffic, the end user(s) originating the traffic are able to demonstrate to you that the traffic complies with applicable United States laws and regulations, please respond via email to me with the description of the traffic, the identity of the customer, and the customer's explanation.
3. As you investigate this matter, please take appropriate action on your network to ensure compliance with applicable United States laws and regulations, and inform me of the action you have taken.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream carriers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call 202-756-6999 or contact me via reply email should you have any questions, or would like to discuss.

Best Regards,

Patrick Halley
Senior Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
<https://traceback.ustelecom.org/Form/Login/r;REDACTED?t=anIIFN1K>
(URL is a private login; do not share.)

Call Details for Incident #2709 (new)

Date/Time:

2020-07-08 15:46:00 UTC

To:

+15752022683

From:

+19152453792

Campaign:

Utility-30MinDisconnect

Likely FRAUD. Recorded message says your electric service will be disconnected in 30 minutes; press 1 to make payment arrangements. Utility company is not identified. Assorted toll-free numbers used as caller-ID.

Call Details for Incident #2708 (6m ago)

Date/Time:

2020-07-08 15:46:00 UTC

To:

+15756492707

From:

+19152453792

Campaign:

Utility-30MinDisconnect

(see description above)

From: traceback-notice@tracebacks.org

To: jrolivarm@gmail.com, noc@smartbiztel.com

Date: 28 Jul 20 02:13 UTC

USTELECOM

THE BROADBAND ASSOCIATION

David Frankel from **Industry Traceback Group** has sent you the following message:

Smartbiz -- Please know that we tried to contact Chock Telecom at alejandro@chocktelecom.com regarding three tracebacks but they did not respond to our emails.

To respond, please leave a COMMENT using the link below.

Submit your response via our secure on-line portal:

<https://traceback.ustelecom.org/Form/Login/r;REDACTED?t=juwxWa&h=12482>

(URL is a private login; do not share.)

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com

Date: 24 Aug 20 20:43 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's Industry Traceback Group (ITG), a private-led and the FCC-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's rules, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls. My contact information is listed below, and I would be more than happy to discuss this request with you.

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

An ITG participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with the TRACED Act and the FCC's rules, USTelecom's ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic. To assist us in our efforts, **we are asking that you respond to this traceback inquiry as soon as possible, but no later than three business days from now.**

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI). Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The Federal Communications Commission (FCC) recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible."

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

We are asking that you submit your response to this inquiry via our secure on-line portal, where you can see additional detail about all traceback requests involving your network.

1. Please investigate the source of this traffic and respond with the identity of the upstream service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, please identify that end user. **We ask that you use the link below to access the portal and use the drop-down selector to provide this information.**
2. If, in investigating this traffic, the end user(s) originating the traffic are able to demonstrate to you that the traffic complies with applicable United States laws and regulations, please provide such information in the comments portion of the applicable traceback, including the identity of the customer and the customer's explanation of such traffic.
3. As you investigate this matter, please take appropriate action on your network to ensure compliance with applicable United States laws and regulations, and indicate what mitigation steps have been taken to prevent such suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends. Please feel free to consult with your counsel on this request, and do not hesitate to contact me via reply email should you have any questions, or would like to discuss.

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:

[Redacted](#)

(URL is a private login; do not share.)

Call Details for Traceback #2930 (new)

Date/Time:2020-08-24 14:40 UTC

Campaign:SSA-P1-BenefitsCanceled (GovtImpers)

Captured recordings suggest these calls are perpetrating a SERIOUS FRAUD. Caller is impersonating a federal official. Automated message threatens that social security benefits will be canceled. Caller-ID appears to be a random toll-free number. Called party is asked to press 1 to speak to an agent. Caller-ID is random (different on each call) so blocking the ANI is not effective. This call is just one example representative of millions of similar calls. Originators please search your records for similar traffic.

From: traceback-notice@tracebacks.org

To: katherine.rosales@smartbiztel.com

Date: 24 Aug 20 20:43 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's Industry Traceback Group (ITG), a private-led and the FCC-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's rules, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls. My contact information is listed below, and I would be more than happy to discuss this request with you.

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

An ITG participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with the TRACED Act and the FCC's rules, USTelecom's ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic. To assist us in our efforts, **we are asking that you respond to this traceback inquiry as soon as possible, but no later than three business days from now.**

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI). Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The Federal Communications Commission (FCC) recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible."

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

We are asking that you submit your response to this inquiry via our secure on-line portal, where you can see additional detail about all traceback requests involving your network.

1. Please investigate the source of this traffic and respond with the identity of the upstream service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, please identify that end user. **We ask that you use the link below to access the portal and use the drop-down selector to provide this information.**
2. If, in investigating this traffic, the end user(s) originating the traffic are able to demonstrate to you that the traffic complies with applicable United States laws and regulations, please provide such information in the comments portion of the applicable traceback, including the identity of the customer and the customer's explanation of such traffic.
3. As you investigate this matter, please take appropriate action on your network to ensure compliance with applicable United States laws and regulations, and indicate what mitigation steps have been taken to prevent such suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends. Please feel free to consult with your counsel on this request, and do not hesitate to contact me via reply email should you have any questions, or would like to discuss.

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:

[Redacted](#)

(URL is a private login; do not share.)

Call Details for Traceback #2930 (new)

Date/Time: 2020-08-24 14:40 UTC

Campaign: SSA-P1-BenefitsCanceled (GovtImpers)

Captured recordings suggest these calls are perpetrating a SERIOUS FRAUD. Caller is impersonating a federal official. Automated message threatens that social security benefits will be canceled. Caller-ID appears to be a random toll-free number. Called party is asked to press 1 to speak to an agent. Caller-ID is random (different on each call) so blocking the ANI is not effective. This call is just one example representative of millions of similar calls. Originators please search your records for similar traffic.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com

Date: 01 Sep 20 18:03 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #2974 (new)

Date/Time: 2020-08-28 22:17 UTC
To: +16158531761
From: +13324567348
Campaign: SSA-P1-BenefitsCanceled (GovtImpers)

Captured recordings suggest these calls are perpetrating a SERIOUS FRAUD. Caller is impersonating a federal official. Automated message threatens that social security benefits will be canceled. Caller-ID appears to be a random toll-free number. Called party is asked to press 1 to speak to an agent. Caller-ID is random (different on each call) so blocking the ANI is not effective. This call is just one example representative of millions of similar calls. Originators please search your records for similar traffic.

From: traceback-notice@tracebacks.org

To: katherine.rosales@smartbiztel.com

Date: 01 Sep 20 18:03 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #2974 (new)

Date/Time:	2020-08-28 22:17 UTC
To:	+16158531761
From:	+13324567348
Campaign:	SSA-P1-BenefitsCanceled (GovtImpers)

Captured recordings suggest these calls are perpetrating a SERIOUS FRAUD. Caller is impersonating a federal official. Automated message threatens that social security benefits will be canceled. Caller-ID appears to be a random toll-free number. Called party is asked to press 1 to speak to an agent. Caller-ID is random (different on each call) so blocking the ANI is not effective. This call is just one example representative of millions of similar calls. Originators please search your records for similar traffic.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com

Date: 11 Sep 20 11:45 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3041 (new)

Date/Time:	2020-09-08 20:33 UTC
To:	+17077243424
From:	+12027732811
Campaign:	SSA-P1-BenefitsCanceled (GovtImpers)

Captured recordings suggest these calls are perpetrating a SERIOUS FRAUD. Caller is impersonating a federal official. Automated message threatens that social security benefits will be canceled. Caller-ID appears to be a random toll-free number. Called party is asked to press 1 to speak to an agent. Caller-ID is random (different on each call) so blocking the ANI is not effective. This call is just one example representative of millions of similar calls. Originators please search your records for similar traffic.

From: traceback-notice@tracebacks.org

To: katherine.rosales@smartbiztel.com

Date: 11 Sep 20 11:45 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3041 (new)

Date/Time:	2020-09-08 20:33 UTC
To:	+17077243424
From:	+12027732811
Campaign:	SSA-P1-BenefitsCanceled (GovtImpers)

Captured recordings suggest these calls are perpetrating a SERIOUS FRAUD. Caller is impersonating a federal official. Automated message threatens that social security benefits will be canceled. Caller-ID appears to be a random toll-free number. Called party is asked to press 1 to speak to an agent. Caller-ID is random (different on each call) so blocking the ANI is not effective. This call is just one example representative of millions of similar calls. Originators please search your records for similar traffic.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com

Date: 16 Sep 20 17:27 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days from now*. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3106 (new)

Date/Time:	2020-09-11 16:36 UTC
To:	+19542708930
From:	+19549446366
Campaign:	Utility-30MinDisconnect

Likely FRAUD. Recorded message says your electric service will be disconnected in 30 minutes; press 1 to make payment arrangements. Utility company is not always identified. Assorted toll-free or other numbers used as caller-ID.

From: traceback-notice@tracebacks.org

To: katherine.rosales@smartbiztel.com

Date: 16 Sep 20 17:27 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3106 (new)

Date/Time:	2020-09-11 16:36 UTC
To:	+19542708930
From:	+19549446366
Campaign:	Utility-30MinDisconnect

Likely FRAUD. Recorded message says your electric service will be disconnected in 30 minutes; press 1 to make payment arrangements. Utility company is not always identified. Assorted toll-free or other numbers used as caller-ID.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com

Date: 23 Sep 20 19:51 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days from now*. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3148 (new)

Date/Time:	2020-09-22 18:26 UTC
To:	+15033801432
From:	+15036725400
Campaign:	Utility-30MinDisconnect

Likely FRAUD. Recorded message says your electric service will be disconnected in 30 minutes; press 1 to make payment arrangements. Utility company is not always identified. Assorted toll-free or other numbers used as caller-ID.

From: traceback-notice@tracebacks.org

To: katherine.rosales@smartbiztel.com

Date: 23 Sep 20 19:51 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days from now*. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3148 (new)

Date/Time:	2020-09-22 18:26 UTC
To:	+15033801432
From:	+15036725400
Campaign:	Utility-30MinDisconnect

Likely FRAUD. Recorded message says your electric service will be disconnected in 30 minutes; press 1 to make payment arrangements. Utility company is not always identified. Assorted toll-free or other numbers used as caller-ID.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com

Date: 25 Sep 20 12:58 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3165 (new)

Date/Time:	2020-09-22 19:14 UTC
To:	+19192800873
From:	+19197032116
Campaign:	Utility-30MinDisconnect - NC

Calls to Duke Energy Customers in North Carolina claiming to be Duke Energy and threatening to shut off recipient's power within 30 minutes for unpaid bills. Potential UDAP and TCPA violations.

From: traceback-notice@tracebacks.org

To: katherine.rosales@smartbiztel.com

Date: 25 Sep 20 12:58 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days from now*. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3165 (new)

Date/Time:	2020-09-22 19:14 UTC
To:	+19192800873
From:	+19197032116
Campaign:	Utility-30MinDisconnect - NC

Calls to Duke Energy Customers in North Carolina claiming to be Duke Energy and threatening to shut off recipient's power within 30 minutes for unpaid bills. Potential UDAP and TCPA violations.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com

Date: 25 Sep 20 15:37 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days from now*. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3164 (new)

Date/Time:	2020-09-23 14:02 UTC
To:	+19192800873
From:	+19193487149
Campaign:	Utility-30MinDisconnect - NC

Calls to Duke Energy Customers in North Carolina claiming to be Duke Energy and threatening to shut off recipient's power within 30 minutes for unpaid bills. Potential UDAP and TCPA violations.

From: traceback-notice@tracebacks.org

To: katherine.rosales@smartbiztel.com

Date: 25 Sep 20 15:37 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3164 (new)

Date/Time:	2020-09-23 14:02 UTC
To:	+19192800873
From:	+19193487149
Campaign:	Utility-30MinDisconnect - NC

Calls to Duke Energy Customers in North Carolina claiming to be Duke Energy and threatening to shut off recipient's power within 30 minutes for unpaid bills. Potential UDAP and TCPA violations.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com

Date: 25 Sep 20 15:55 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days from now*. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3167 (new)

Date/Time:	2020-09-23 17:05 UTC
To:	+17042800080
From:	+17047621511
Campaign:	Utility-30MinDisconnect - NC

Calls to Duke Energy Customers in North Carolina claiming to be Duke Energy and threatening to shut off recipient's power within 30 minutes for unpaid bills. Potential UDAP and TCPA violations.

From: traceback-notice@tracebacks.org

To: katherine.rosales@smartbiztel.com

Date: 25 Sep 20 15:55 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days from now*. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3167 (new)

Date/Time:	2020-09-23 17:05 UTC
To:	+17042800080
From:	+17047621511
Campaign:	Utility-30MinDisconnect - NC

Calls to Duke Energy Customers in North Carolina claiming to be Duke Energy and threatening to shut off recipient's power within 30 minutes for unpaid bills. Potential UDAP and TCPA violations.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com

Date: 25 Sep 20 17:49 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3169 (new)

Date/Time:	2020-09-23 17:11 UTC
To:	+17042800080
From:	+17046091598
Campaign:	Utility-30MinDisconnect - NC

Calls to Duke Energy Customers in North Carolina claiming to be Duke Energy and threatening to shut off recipient's power within 30 minutes for unpaid bills. Potential UDAP and TCPA violations.

From: traceback-notice@tracebacks.org

To: katherine.rosales@smartbiztel.com

Date: 25 Sep 20 17:49 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3169 (new)

Date/Time:	2020-09-23 17:11 UTC
To:	+17042800080
From:	+17046091598
Campaign:	Utility-30MinDisconnect - NC

Calls to Duke Energy Customers in North Carolina claiming to be Duke Energy and threatening to shut off recipient's power within 30 minutes for unpaid bills. Potential UDAP and TCPA violations.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com

Date: 30 Sep 20 19:36 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days from now*. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3210 (new)

Date/Time:	2020-09-24 15:02 UTC
To:	+15105206394
From:	+19152680196
Campaign:	USTreas-SSA-EnforceAction (GovtImpers)

FRAUD. Claims to be from US Treasury regarding an enforcement action. Impersonates a government official. Recorded/automated voice to wireless numbers generally prohibited. Random spoofing of Caller-ID. Blocking the ANI is not effective.

From: traceback-notice@tracebacks.org

To: katherine.rosales@smartbiztel.com

Date: 30 Sep 20 19:36 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3210 (new)

Date/Time:	2020-09-24 15:02 UTC
To:	+15105206394
From:	+19152680196
Campaign:	USTreas-SSA-EnforceAction (GovtImpers)

FRAUD. Claims to be from US Treasury regarding an enforcement action. Impersonates a government official. Recorded/automated voice to wireless numbers generally prohibited. Random spoofing of Caller-ID. Blocking the ANI is not effective.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com

Date: 30 Sep 20 20:15 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days from now*. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3213 (new)

Date/Time: 2020-09-30 16:07 UTC
To: +15866152626
From: +15865546987
Campaign: Utility-30MinDisconnect

Likely FRAUD. Recorded message says your electric service will be disconnected in 30 minutes; press 1 to make payment arrangements. Utility company is not always identified. Assorted toll-free or other numbers used as caller-ID.

From: traceback-notice@tracebacks.org

To: katherine.rosales@smartbiztel.com

Date: 30 Sep 20 20:15 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3213 (new)

Date/Time: 2020-09-30 16:07 UTC
To: +15866152626
From: +15865546987
Campaign: Utility-30MinDisconnect

Likely FRAUD. Recorded message says your electric service will be disconnected in 30 minutes; press 1 to make payment arrangements. Utility company is not always identified. Assorted toll-free or other numbers used as caller-ID.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com

Date: 03 Oct 20 09:55 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3242 (new)	
Date/Time:	2020-09-30 16:52 UTC
To:	+17082127770
From:	+12125341961
Campaign:	BofA - Chinese Voice Department
Confirmed fraudulent call, identifying the calling party as Bank of America's Chinese Voice Dept. Recorded voice in foreign language.	

From: traceback-notice@tracebacks.org

To: katherine.rosales@smartbiztel.com

Date: 03 Oct 20 09:56 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3242 (new)	
Date/Time:	2020-09-30 16:52 UTC
To:	+17082127770
From:	+12125341961
Campaign:	BofA - Chinese Voice Department
Confirmed fraudulent call, identifying the calling party as Bank of America's Chinese Voice Dept. Recorded voice in foreign language.	

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com

Date: 06 Oct 20 16:31 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3253 (new)

Date/Time: 2020-10-05 15:39 UTC
To: +12604501996
From: +14438898013
Campaign: Utility-30MinDisconnect

Likely FRAUD. Recorded message says your electric service will be disconnected in 30 minutes; press 1 to make payment arrangements. Utility company is not always identified. Assorted toll-free or other numbers used as caller-ID.

From: traceback-notice@tracebacks.org

To: katherine.rosales@smartbiztel.com

Date: 06 Oct 20 16:31 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days from now*. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3253 (new)

Date/Time: 2020-10-05 15:39 UTC
To: +12604501996
From: +14438898013
Campaign: Utility-30MinDisconnect

Likely FRAUD. Recorded message says your electric service will be disconnected in 30 minutes; press 1 to make payment arrangements. Utility company is not always identified. Assorted toll-free or other numbers used as caller-ID.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 10 Oct 20 11:11 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3278 (new)

Date/Time:	2020-10-09 15:12 UTC
To:	+18329745040
From:	+16107707265
Campaign:	Refund-ComputerServices

FRAUD. Recorded message claims that a computer services subscription renewal fee of 399 has been charged to your account. Recorded message to wireless number generally not allowed. Calling party must be identified in voice-mail. Claimed subscription does not exist. Call is FRAUD.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 10 Oct 20 11:16 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3281 (new)

Date/Time:	2020-10-09 19:18 UTC
To:	+15854290867
From:	+16318239445
Campaign:	SSA-P1-TexasFraud (GovtImpers)

FRAUD. Recorded message says SSN is suspended due to fraud in Texas or other state. Caller fraudulently claims to be from SSA. Spoofed caller-ID using random wireless and other USA subscriber numbers.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 12 Oct 20 14:47 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3280 (new)

Date/Time:	2020-10-09 19:07 UTC
To:	+14058378238
From:	+16314928412
Campaign:	SSA-P1-TexasFraud (GovtImpers)

FRAUD. Recorded message says SSN is suspended due to fraud in Texas or other state. Caller fraudulently claims to be from SSA. Spoofed caller-ID using random wireless and other USA subscriber numbers.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 13 Oct 20 13:46 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3286 (new)

Date/Time:	2020-10-12 17:09 UTC
To:	+12298699355
From:	+17064746058
Campaign:	Utility-30MinDisconnect

Likely FRAUD. Recorded message says your electric service will be disconnected in 30 minutes; press 1 to make payment arrangements. Utility company is not always identified. Assorted toll-free or other numbers used as caller-ID.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 13 Oct 20 16:38 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3295 (new)

Date/Time:	2020-09-23 10:54 UTC
To:	+19192803863
From:	+19196444369
Campaign:	Utility-30MinDisconnect - NC

Calls to Duke Energy Customers in North Carolina claiming to be Duke Energy and threatening to shut off recipient's power within 30 minutes for unpaid bills. Potential UDAP and TCPA violations.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 14 Oct 20 21:27 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3305 (new)

Date/Time:	2020-10-01 18:37 UTC
To:	+16309145221
From:	+12108661809
Campaign:	SSA-Various (GovtImpers)

These calls fraudulently claim to be from US Social Security Administration, threatening problems with SS account. Calling number may be a spoofed toll-free number, or a call-back number. These incidents may be from separate campaigns.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 14 Oct 20 21:28 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3313 (new)

Date/Time:	2020-10-09 22:46 UTC
To:	+13172925853
From:	+13172560188
Campaign:	SSA-P1-TexasFraud (GovtImpers)

FRAUD. Recorded message says SSN is suspended due to fraud in Texas or other state. Caller fraudulently claims to be from SSA. Spoofed caller-ID using random wireless and other USA subscriber numbers.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 16 Oct 20 20:50 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3329 (new)

Date/Time:	2020-10-16 17:54 UTC
To:	+17205766948
From:	+17205768527
Campaign:	SSA-P1-BenefitsCanceled (GovtImpers)

Captured recordings suggest these calls are perpetrating a SERIOUS FRAUD. Caller is impersonating a federal official. Automated message threatens that social security benefits will be canceled. Caller-ID appears to be a random toll-free number. Called party is asked to press 1 to speak to an agent. Caller-ID is random (different on each call) so blocking the ANI is not effective. This call is just one example representative of millions of similar calls. Originators please search your records for similar traffic.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 19 Oct 20 14:59 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3338 (new)

Date/Time: 2020-10-14 21:46 UTC
To: +14343340431
From: +14347286018
Campaign: Utility-30MinDisconnect

Likely FRAUD. Recorded message says your electric service will be disconnected in 30 minutes; press 1 to make payment arrangements. Utility company is not always identified. Assorted toll-free or other numbers used as caller-ID.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 19 Oct 20 16:40 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3339 (new)	
Date/Time:	2020-10-16 19:43 UTC
To:	+17323221263
From:	+18003582090
Campaign:	BofA - Chinese Voice Department
Confirmed fraudulent call, identifying the calling party as Bank of America's Chinese Voice Dept. Recorded voice in foreign language.	

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 19 Oct 20 19:45 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3336 (new)

Date/Time: 2020-10-16 17:43 UTC
To: +13053455600
From: +15616278328
Campaign: Utility-30MinDisconnect

Likely FRAUD. Recorded message says your electric service will be disconnected in 30 minutes; press 1 to make payment arrangements. Utility company is not always identified. Assorted toll-free or other numbers used as caller-ID.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 21 Oct 20 19:15 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3375 (new)	
Date/Time:	2020-10-21 15:59 UTC
To:	+12196702513
From:	+14078961571
Campaign:	Apple-iCloud-AccountBreached
Caller identifies themselves as calling on behalf of Apple and claims the called party's iCloud account has been breached.	

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 21 Oct 20 22:12 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3378 (new)

Date/Time:	2020-10-21 11:35 UTC
To:	+17275885222
From:	+12023673346
Campaign:	TDoS - Hospital ER Oct 21

Urgent. Active TDoS attack affecting major hospital, disrupting emergency room lines.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 22 Oct 20 19:40 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3388 (new)

Date/Time: 2020-10-22 15:31 UTC
To: +12099689504
From: +15107196474
Campaign: Utility-30MinDisconnect

Likely FRAUD. Recorded message says your electric service will be disconnected in 30 minutes; press 1 to make payment arrangements. Utility company is not always identified. Assorted toll-free or other numbers used as caller-ID.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 22 Oct 20 19:56 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3386 (new)

Date/Time:	2020-10-22 16:22 UTC
To:	+17042362946
From:	+19805805052
Campaign:	Utility-30MinDisconnect

Likely FRAUD. Recorded message says your electric service will be disconnected in 30 minutes; press 1 to make payment arrangements. Utility company is not always identified. Assorted toll-free or other numbers used as caller-ID.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 23 Oct 20 16:04 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3387 (new)

Date/Time:	2020-10-21 15:34 UTC
To:	+14154207123
From:	+14156645662
Campaign:	Utility-30MinDisconnect

Likely FRAUD. Recorded message says your electric service will be disconnected in 30 minutes; press 1 to make payment arrangements. Utility company is not always identified. Assorted toll-free or other numbers used as caller-ID.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 27 Oct 20 22:28 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3424 (new)

Date/Time: 2020-10-27 18:24 UTC
To: +19166061486
From: +14155675039
Campaign: Utility-30MinDisconnect

Likely FRAUD. Recorded message says your electric service will be disconnected in 30 minutes; press 1 to make payment arrangements. Utility company is not always identified. Assorted toll-free or other numbers used as caller-ID.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 28 Oct 20 00:29 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3427 (new)

Date/Time: 2020-10-27 17:09 UTC
To: +12162722601
From: +14782366213
Campaign: SSA-P1-TexasFraud (GovtImpers)

FRAUD. Recorded message says SSN is suspended due to fraud in Texas or other state. Caller fraudulently claims to be from SSA. Spoofed caller-ID using random wireless and other USA subscriber numbers.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 30 Oct 20 12:52 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3449 (new)

Date/Time: 2020-10-29 16:08 UTC

To: +13092368670

From: +13092368963

Campaign: Apple-iCloud-AccountBreachd

Caller identifies themselves as calling on behalf of Apple and claims the called party's iCloud account has been breached.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 30 Oct 20 21:16 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3467 (new)

Date/Time: 2020-10-30 07:15 UTC
To: +15592071345
From: +15595542972
Campaign: Utility-30MinDisconnect

Likely FRAUD. Recorded message says your electric service will be disconnected in 30 minutes; press 1 to make payment arrangements. Utility company is not always identified. Assorted toll-free or other numbers used as caller-ID.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 01 Nov 20 23:55 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3470 (new)

Date/Time: 2020-10-30 18:13 UTC
To: +19704434520
From: +13257627039
Campaign: SSA-CalltheSSA

FRAUD. Recorded message says SSN is suspended due to law enforcement action. Caller fraudulently claims to be from SSA. Spoofed caller-ID using random wireless and other USA subscriber numbers.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 02 Nov 20 15:24 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3469 (new)

Date/Time: 2020-10-30 16:59 UTC
To: +19015901527
From: +19014227394
Campaign: Utility-30MinDisconnect

Likely FRAUD. Recorded message says your electric service will be disconnected in 30 minutes; press 1 to make payment arrangements. Utility company is not always identified. Assorted toll-free or other numbers used as caller-ID.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 03 Nov 20 18:50 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3491 (new)

Date/Time: 2020-11-03 14:29 UTC
To: +19174744614
From: +19174746959
Campaign: TestCall-StaySafeStayHome

Artificial voice announces "Hello. This is just a test call. Time to stay home. Stay safe and stay home." Automated calls to wireless numbers not permitted. Caller-ID is spoofed without permission. Caller does not identify source of call or provide opt-out. High-volume campaign.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 04 Nov 20 20:48 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3500 (new)

Date/Time: 2020-11-04 14:17 UTC
To: +19192705765
From: +19192704271
Campaign: TestCall-StaySafeStayHome

Artificial voice announces "Hello. This is just a test call. Time to stay home. Stay safe and stay home." Automated calls to wireless numbers not permitted. Caller-ID is spoofed without permission. Caller does not identify source of call or provide opt-out. High-volume campaign.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 05 Nov 20 13:08 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3502 (new)

Date/Time: 2020-11-04 21:45 UTC
To: +14043331612
From: +14235248069
Campaign: SSA-P1-TexasFraud (GovtImpers)

FRAUD. Recorded message says SSN is suspended due to fraud in Texas or other state. Caller fraudulently claims to be from SSA. Spoofed caller-ID using random wireless and other USA subscriber numbers.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 06 Nov 20 12:35 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3515 (new)

Date/Time: 2020-11-03 20:23 UTC
To: +16107015671
From: +14232051615
Campaign: TestCall-StaySafeStayHome

Artificial voice announces "Hello. This is just a test call. Time to stay home. Stay safe and stay home." Automated calls to wireless numbers not permitted. Caller-ID is spoofed without permission. Caller does not identify source of call or provide opt-out. High-volume campaign.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 06 Nov 20 12:36 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3516 (new)

Date/Time: 2020-11-03 20:22 UTC
To: +17704573716
From: +14232051615
Campaign: TestCall-StaySafeStayHome

Artificial voice announces "Hello. This is just a test call. Time to stay home. Stay safe and stay home." Automated calls to wireless numbers not permitted. Caller-ID is spoofed without permission. Caller does not identify source of call or provide opt-out. High-volume campaign.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 06 Nov 20 13:27 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3520 (new)

Date/Time: 2020-11-05 17:32 UTC
To: +18454222234
From: +18454522713
Campaign: Utility-30MinDisconnect

Likely FRAUD. Recorded message says your electric service will be disconnected in 30 minutes; press 1 to make payment arrangements. Utility company is not always identified. Assorted toll-free or other numbers used as caller-ID.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 06 Nov 20 18:35 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3532 (new)

Date/Time: 2020-11-06 17:28 UTC

To: +14843402875

From: +14078567877

Campaign: Apple-iCloud-AccountBreached

Caller identifies themselves as calling on behalf of Apple and claims the called party's iCloud account has been breached.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 06 Nov 20 19:48 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3538 (new)

Date/Time: 2020-11-05 17:12 UTC
To: +16189677570
From: +16189676967
Campaign: CCIRR - VisaAlert

FRAUD. Automated voice offering zero percent interest rate, identified as the alert system with Visa MasterCard Account Services. Caller ID is spoofed with a random NPA so blocking the ANI is not effective. Many caller-IDs are invalid. Millions of calls daily. Calls are illegal because they are automated calls to mobiles, they use improper caller-ID, they do not identify the caller at the beginning of the message, they do not give an operable call-back number. This call is just one example of millions of similar calls. Originators please search your records for similar traffic and address with your customer.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 06 Nov 20 20:58 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3534 (new)

Date/Time: 2020-11-06 17:33 UTC
To: +12016180263
From: +17108854973
Campaign: SSA-P1-TexasFraud (GovtImpers)

FRAUD. Recorded message says SSN is suspended due to fraud in Texas or other state. Caller fraudulently claims to be from SSA. Spoofed caller-ID using random wireless and other USA subscriber numbers.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 06 Nov 20 21:09 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3539 (new)

Date/Time: 2020-11-06 15:48 UTC
To: +12148039575
From: +14696460814
Campaign: Utility-30MinDisconnect

Likely FRAUD. Recorded message says your electric service will be disconnected in 30 minutes; press 1 to make payment arrangements. Utility company is not always identified. Assorted toll-free or other numbers used as caller-ID.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 09 Nov 20 11:08 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3517 (new)

Date/Time: 2020-11-02 23:45 UTC
To: +18282565324
From: +14232051615
Campaign: TestCall-StaySafeStayHome

Artificial voice announces "Hello. This is just a test call. Time to stay home. Stay safe and stay home." Automated calls to wireless numbers not permitted. Caller-ID is spoofed without permission. Caller does not identify source of call or provide opt-out. High-volume campaign.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 10 Nov 20 16:08 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3562 (new)

Date/Time: 2020-11-10 14:45 UTC
To: +17733831213
From: +17733834307
Campaign: TestCall-StaySafeStayHome

Artificial voice announces "Hello. This is just a test call. Time to stay home. Stay safe and stay home." Automated calls to wireless numbers not permitted. Caller-ID is spoofed without permission. Caller does not identify source of call or provide opt-out. High-volume campaign.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 16 Nov 20 14:22 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3601 (new)

Date/Time: 2020-11-13 14:37 UTC
To: +13472676025
From: +12176525064
Campaign: TestCall-StaySafeStayHome

Artificial voice announces "Hello. This is just a test call. Time to stay home. Stay safe and stay home." Automated calls to wireless numbers not permitted. Caller-ID is spoofed without permission. Caller does not identify source of call or provide opt-out. High-volume campaign.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 16 Nov 20 18:18 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3609 (new)

Date/Time: 2020-11-12 17:15 UTC
To: +13146144114
From: +13143607443
Campaign: Utility-30MinDisconnect

Likely FRAUD. Recorded message says your electric service will be disconnected in 30 minutes; press 1 to make payment arrangements. Utility company is not always identified. Assorted toll-free or other numbers used as caller-ID.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 16 Nov 20 20:34 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3596 (new)

Date/Time: 2020-11-12 19:32 UTC
To: +13369728109
From: +15614851173
Campaign: SSA-CalltheSSA

FRAUD. Recorded message says SSN is suspended due to law enforcement action. Caller fraudulently claims to be from SSA. Spoofed caller-ID using random wireless and other USA subscriber numbers.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 16 Nov 20 23:42 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days from now*. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3618 (new)

Date/Time: 2020-11-16 20:56 UTC
To: +18176756520
From: +18176681937
Campaign: SSA-P1-TexasFraud (GovtImpers)

FRAUD. Recorded message says SSN is suspended due to fraud in Texas or other state. Caller fraudulently claims to be from SSA. Spoofed caller-ID using random wireless and other USA subscriber numbers.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 19 Nov 20 15:32 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3637 (new)

Date/Time: 2020-11-18 17:26 UTC

To: +16082091407

From: +18667636020

Campaign: Apple-iCloud-AccountBreached

Caller identifies themselves as calling on behalf of Apple and claims the called party's iCloud account has been breached.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 19 Nov 20 18:31 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3648 (new)

Date/Time: 2020-11-19 14:54 UTC
To: +12013068860
From: +15162916551
Campaign: SSA-P1-TexasFraud (GovtImpers)

FRAUD. Recorded message says SSN is suspended due to fraud in Texas or other state. Caller fraudulently claims to be from SSA. Spoofed caller-ID using random wireless and other USA subscriber numbers.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 19 Nov 20 18:56 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3638 (new)

Date/Time: 2020-11-18 17:16 UTC

To: +19099382089

From: +18668969240

Campaign: Apple-iCloud-AccountBreached

Caller identifies themselves as calling on behalf of Apple and claims the called party's iCloud account has been breached.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 23 Nov 20 16:50 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days from now*. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3666 (new)

Date/Time: 2020-11-23 14:33 UTC
To: +14438441585
From: +14438446982
Campaign: TestCall-StaySafeStayHome

Artificial voice announces "Hello. This is just a test call. Time to stay home. Stay safe and stay home." Automated calls to wireless numbers not permitted. Caller-ID is spoofed without permission. Caller does not identify source of call or provide opt-out. High-volume campaign.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 23 Nov 20 18:08 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3655 (new)

Date/Time: 2020-11-20 15:01 UTC
To: +14436943211
From: +14436945790
Campaign: TestCall-StaySafeStayHome

Artificial voice announces "Hello. This is just a test call. Time to stay home. Stay safe and stay home." Automated calls to wireless numbers not permitted. Caller-ID is spoofed without permission. Caller does not identify source of call or provide opt-out. High-volume campaign.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 23 Nov 20 22:35 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3630 (new)

Date/Time: 2020-11-18 17:30 UTC
To: +13023896918
From: +13023896557
Campaign: TestCall-StaySafeStayHome

Artificial voice announces "Hello. This is just a test call. Time to stay home. Stay safe and stay home." Automated calls to wireless numbers not permitted. Caller-ID is spoofed without permission. Caller does not identify source of call or provide opt-out. High-volume campaign.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 30 Nov 20 19:05 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3732 (new)

Date/Time: 2020-11-30 15:56 UTC
To: +17737937445
From: +17737935234
Campaign: TestCall-StaySafeStayHome

Artificial voice announces "Hello. This is just a test call. Time to stay home. Stay safe and stay home." Automated calls to wireless numbers not permitted. Caller-ID is spoofed without permission. Caller does not identify source of call or provide opt-out. High-volume campaign.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 30 Nov 20 19:07 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3733 (new)

Date/Time: 2020-11-30 14:54 UTC
To: +17735529330
From: +13230291988
Campaign: TestCall-StaySafeStayHome

Artificial voice announces "Hello. This is just a test call. Time to stay home. Stay safe and stay home." Automated calls to wireless numbers not permitted. Caller-ID is spoofed without permission. Caller does not identify source of call or provide opt-out. High-volume campaign.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 01 Dec 20 18:19 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3743 (new)

Date/Time: 2020-12-01 15:00 UTC
To: +13023592189
From: +13023595927
Campaign: TestCall-StaySafeStayHome

Artificial voice announces "Hello. This is just a test call. Time to stay home. Stay safe and stay home." Automated calls to wireless numbers not permitted. Caller-ID is spoofed without permission. Caller does not identify source of call or provide opt-out. High-volume campaign.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 01 Dec 20 18:24 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3744 (new)

Date/Time: 2020-12-01 15:48 UTC
To: +14432069348
From: +14432066487
Campaign: TestCall-StaySafeStayHome

Artificial voice announces "Hello. This is just a test call. Time to stay home. Stay safe and stay home." Automated calls to wireless numbers not permitted. Caller-ID is spoofed without permission. Caller does not identify source of call or provide opt-out. High-volume campaign.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 02 Dec 20 14:59 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3726 (new)

Date/Time: 2020-11-25 23:55 UTC
To: +18458254286
From: +18458853318
Campaign: SSA-P1-TexasFraud (GovtImpers)

FRAUD. Recorded message says SSN is suspended due to fraud in Texas or other state. Caller fraudulently claims to be from SSA. Spoofed caller-ID using random wireless and other USA subscriber numbers.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 02 Dec 20 18:03 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3746 (new)

Date/Time: 2020-12-02 15:22 UTC
To: +16187511462
From: +16187515058
Campaign: TestCall-StaySafeStayHome

Artificial voice announces "Hello. This is just a test call. Time to stay home. Stay safe and stay home." Automated calls to wireless numbers not permitted. Caller-ID is spoofed without permission. Caller does not identify source of call or provide opt-out. High-volume campaign.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 03 Dec 20 12:57 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3753 (new)

Date/Time: 2020-12-02 16:55 UTC

To: +14802664201

From: +18445779802

Campaign: Apple-iCloud-AccountBreached

Caller identifies themselves as calling on behalf of Apple and claims the called party's iCloud account has been breached.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 03 Dec 20 17:07 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3737 (new)

Date/Time: 2020-11-30 18:32 UTC
To: +17707228370
From: +16122490528
Campaign: SSA-CalltheSSA

FRAUD. Recorded message says SSN is suspended due to law enforcement action. Caller fraudulently claims to be from SSA. Spoofed caller-ID using random wireless and other USA subscriber numbers.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 04 Dec 20 20:41 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3778 (new)

Date/Time: 2020-12-04 13:48 UTC
To: +19418076936
From: +12029672853
Campaign: SSA-CalltheSSA

FRAUD. Recorded message says SSN is suspended due to law enforcement action. Caller fraudulently claims to be from SSA. Spoofed caller-ID using random wireless and other USA subscriber numbers.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 07 Dec 20 19:50 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3788 (new)

Date/Time: 2020-12-07 14:41 UTC
To: +19495334560
From: +19495173562
Campaign: TestCall-StaySafeStayHome

Artificial voice announces "Hello. This is just a test call. Time to stay home. Stay safe and stay home." Automated calls to wireless numbers not permitted. Caller-ID is spoofed without permission. Caller does not identify source of call or provide opt-out. High-volume campaign.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 08 Dec 20 16:40 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3799 (new)

Date/Time: 2020-12-08 14:58 UTC
To: +17347298520
From: +17345598728
Campaign: TestCall-StaySafeStayHome

Artificial voice announces "Hello. This is just a test call. Time to stay home. Stay safe and stay home." Automated calls to wireless numbers not permitted. Caller-ID is spoofed without permission. Caller does not identify source of call or provide opt-out. High-volume campaign.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 09 Dec 20 15:42 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3801 (new)

Date/Time: 2020-12-09 14:32 UTC
To: +13023592189
From: +13025088586
Campaign: TestCall-StaySafeStayHome

Artificial voice announces "Hello. This is just a test call. Time to stay home. Stay safe and stay home." Automated calls to wireless numbers not permitted. Caller-ID is spoofed without permission. Caller does not identify source of call or provide opt-out. High-volume campaign.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 09 Dec 20 19:07 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3803 (new)

Date/Time: 2020-12-09 14:35 UTC
To: +13136159207
From: +13135801847
Campaign: TestCall-StaySafeStayHome

Artificial voice announces "Hello. This is just a test call. Time to stay home. Stay safe and stay home." Automated calls to wireless numbers not permitted. Caller-ID is spoofed without permission. Caller does not identify source of call or provide opt-out. High-volume campaign.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 09 Dec 20 22:46 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3802 (new)

Date/Time: 2020-12-09 14:49 UTC
To: +13014015722
From: +13015904251
Campaign: TestCall-StaySafeStayHome

Artificial voice announces "Hello. This is just a test call. Time to stay home. Stay safe and stay home." Automated calls to wireless numbers not permitted. Caller-ID is spoofed without permission. Caller does not identify source of call or provide opt-out. High-volume campaign.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 10 Dec 20 02:16 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3798 (new)

Date/Time: 2020-12-08 14:54 UTC
To: +13014716299
From: +13015173009
Campaign: TestCall-StaySafeStayHome

Artificial voice announces "Hello. This is just a test call. Time to stay home. Stay safe and stay home." Automated calls to wireless numbers not permitted. Caller-ID is spoofed without permission. Caller does not identify source of call or provide opt-out. High-volume campaign.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 10 Dec 20 17:58 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3808 (new)

Date/Time: 2020-12-09 17:04 UTC

To: +12032571147

From: +12032573662

Campaign: Apple-iCloud-AccountBreached

Caller identifies themselves as calling on behalf of Apple and claims the called party's iCloud account has been breached.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 10 Dec 20 18:49 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3816 (new)

Date/Time: 2020-12-10 15:39 UTC
To: +14109780435
From: +14105851716
Campaign: TestCall-StaySafeStayHome

Artificial voice announces "Hello. This is just a test call. Time to stay home. Stay safe and stay home." Automated calls to wireless numbers not permitted. Caller-ID is spoofed without permission. Caller does not identify source of call or provide opt-out. High-volume campaign.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 10 Dec 20 21:40 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3818 (new)

Date/Time: 2020-12-10 15:02 UTC
To: +15803706720
From: +15806883261
Campaign: TestCall-StaySafeStayHome

Artificial voice announces "Hello. This is just a test call. Time to stay home. Stay safe and stay home." Automated calls to wireless numbers not permitted. Caller-ID is spoofed without permission. Caller does not identify source of call or provide opt-out. High-volume campaign.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 11 Dec 20 15:24 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3813 (new)

Date/Time: 2020-12-09 21:15 UTC
To: +15126325341
From: +15126324456
Campaign: SSA-P1-TexasFraud (GovtImpers)

FRAUD. Recorded message says SSN is suspended due to fraud in Texas or other state. Caller fraudulently claims to be from SSA. Spoofed caller-ID using random wireless and other USA subscriber numbers.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 11 Dec 20 15:54 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3804 (new)

Date/Time: 2020-12-09 20:40 UTC
To: +14075924535
From: +16155517603
Campaign: SSA-CalltheSSA

FRAUD. Recorded message says SSN is suspended due to law enforcement action. Caller fraudulently claims to be from SSA. Spoofed caller-ID using random wireless and other USA subscriber numbers.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 11 Dec 20 20:40 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3837 (new)

Date/Time: 2020-12-11 16:06 UTC
To: +12253646147
From: +12253125463
Campaign: SSA-P1-TexasFraud (GovtImpers)

FRAUD. Recorded message says SSN is suspended due to fraud in Texas or other state. Caller fraudulently claims to be from SSA. Spoofed caller-ID using random wireless and other USA subscriber numbers.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 11 Dec 20 20:41 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3821 (new)

Date/Time: 2020-12-11 14:44 UTC
To: +14433869280
From: +14436118385
Campaign: TestCall-StaySafeStayHome

Artificial voice announces "Hello. This is just a test call. Time to stay home. Stay safe and stay home." Automated calls to wireless numbers not permitted. Caller-ID is spoofed without permission. Caller does not identify source of call or provide opt-out. High-volume campaign.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 14 Dec 20 22:20 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3847 (new)

Date/Time: 2020-12-14 16:40 UTC

To: +13214394256

From: +18775698765

Campaign: Apple-iCloud-AccountBreached

Caller identifies themselves as calling on behalf of Apple and claims the called party's iCloud account has been breached.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 14 Dec 20 22:23 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3831 (new)

Date/Time: 2020-12-11 16:41 UTC
To: +12528221732
From: +16155517549
Campaign: SSA-CalltheSSA

FRAUD. Recorded message says SSN is suspended due to law enforcement action. Caller fraudulently claims to be from SSA. Spoofed caller-ID using random wireless and other USA subscriber numbers.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 15 Dec 20 14:36 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days from now*. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3838 (new)

Date/Time: 2020-12-14 14:51 UTC
To: +14147649957
From: +14146305374
Campaign: TestCall-StaySafeStayHome

Artificial voice announces "Hello. This is just a test call. Time to stay home. Stay safe and stay home." Automated calls to wireless numbers not permitted. Caller-ID is spoofed without permission. Caller does not identify source of call or provide opt-out. High-volume campaign.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 15 Dec 20 20:04 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3856 (new)

Date/Time: 2020-12-15 13:12 UTC
To: +17404858614
From: +17405587922
Campaign: TestCall-StaySafeStayHome

Artificial voice announces "Hello. This is just a test call. Time to stay home. Stay safe and stay home." Automated calls to wireless numbers not permitted. Caller-ID is spoofed without permission. Caller does not identify source of call or provide opt-out. High-volume campaign.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 16 Dec 20 18:27 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3870 (new)

Date/Time: 2020-12-16 16:05 UTC
To: +12165342312
From: +12165311746
Campaign: TestCall-StaySafeStayHome

Artificial voice announces "Hello. This is just a test call. Time to stay home. Stay safe and stay home." Automated calls to wireless numbers not permitted. Caller-ID is spoofed without permission. Caller does not identify source of call or provide opt-out. High-volume campaign.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 18 Dec 20 21:39 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3889 (new)

Date/Time: 2020-12-18 17:00 UTC
To: +13107539888
From: +13103544768
Campaign: TestCall-StaySafeStayHome

Artificial voice announces "Hello. This is just a test call. Time to stay home. Stay safe and stay home." Automated calls to wireless numbers not permitted. Caller-ID is spoofed without permission. Caller does not identify source of call or provide opt-out. High-volume campaign.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 22 Dec 20 19:07 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3913 (new)

Date/Time: 2020-12-21 22:46 UTC

To: +19407660640

From: +19858732466

Campaign: Apple-iCloud-AccountBreached

Caller identifies themselves as calling on behalf of Apple and claims the called party's iCloud account has been breached.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 22 Dec 20 19:09 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3902 (new)

Date/Time: 2020-12-22 15:49 UTC
To: +14065702116
From: +14064644770
Campaign: TestCall-StaySafeStayHome

Artificial voice announces "Hello. This is just a test call. Time to stay home. Stay safe and stay home." Automated calls to wireless numbers not permitted. Caller-ID is spoofed without permission. Caller does not identify source of call or provide opt-out. High-volume campaign.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 23 Dec 20 20:56 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3925 (new)

Date/Time: 2020-12-23 17:02 UTC
To: +17737102238
From: +17735394273
Campaign: TestCall-StaySafeStayHome

Artificial voice announces "Hello. This is just a test call. Time to stay home. Stay safe and stay home." Automated calls to wireless numbers not permitted. Caller-ID is spoofed without permission. Caller does not identify source of call or provide opt-out. High-volume campaign.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 30 Dec 20 11:53 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3901 (new)

Date/Time: 2020-12-22 14:20 UTC
To: +12487705626
From: +12486358481
Campaign: TestCall-StaySafeStayHome

Artificial voice announces "Hello. This is just a test call. Time to stay home. Stay safe and stay home." Automated calls to wireless numbers not permitted. Caller-ID is spoofed without permission. Caller does not identify source of call or provide opt-out. High-volume campaign.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 06 Jan 21 16:28 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days from now*. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #3978 (new)

Date/Time: 2021-01-05 14:40 UTC
To: +12193639044
From: +12194155763
Campaign: TestCall-StaySafeStayHome

Artificial voice announces "Hello. This is just a test call. Time to stay home. Stay safe and stay home." Automated calls to wireless numbers not permitted. Caller-ID is spoofed without permission. Caller does not identify source of call or provide opt-out. High-volume campaign.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 11 Jan 21 17:27 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #4029 (new)

Date/Time: 2021-01-11 14:09 UTC
To: +18155096406
From: +18154141578
Campaign: TestCall-StaySafeStayHome

Artificial voice announces "Hello. This is just a test call. Time to stay home. Stay safe and stay home." Automated calls to wireless numbers not permitted. Caller-ID is spoofed without permission. Caller does not identify source of call or provide opt-out. High-volume campaign.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 11 Jan 21 19:30 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #4027 (new)

Date/Time: 2021-01-10 17:12 UTC

To: +15033691774

From: +15033693771

Campaign: Apple-iCloud-AccountBreached

Caller identifies themselves as calling on behalf of Apple and claims the called party's iCloud account has been breached.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 12 Jan 21 15:51 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #4041 (new)

Date/Time: 2021-01-12 14:12 UTC
To: +17066277556
From: +17066014816
Campaign: TestCall-StaySafeStayHome

Artificial voice announces "Hello. This is just a test call. Time to stay home. Stay safe and stay home." Automated calls to wireless numbers not permitted. Caller-ID is spoofed without permission. Caller does not identify source of call or provide opt-out. High-volume campaign.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 12 Jan 21 16:47 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #4043 (new)

Date/Time: 2021-01-12 14:27 UTC
To: +18062245984
From: +18065849489
Campaign: TestCall-StaySafeStayHome

Artificial voice announces "Hello. This is just a test call. Time to stay home. Stay safe and stay home." Automated calls to wireless numbers not permitted. Caller-ID is spoofed without permission. Caller does not identify source of call or provide opt-out. High-volume campaign.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 14 Jan 21 22:14 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #4067 (new)

Date/Time: 2021-01-14 15:24 UTC
To: +18583492445
From: +19152003833
Campaign: SSA-CalltheSSA

FRAUD. Recorded message says SSN is suspended due to law enforcement action. Caller fraudulently claims to be from SSA. Spoofed caller-ID using random wireless and other USA subscriber numbers.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 26 Jan 21 14:44 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #4154 (new)

Date/Time: 2021-01-25 18:29 UTC
To: +16302050658
From: +14433967696
Campaign: SSA-CalltheSSA

FRAUD. Recorded message says SSN is suspended due to law enforcement action. Caller fraudulently claims to be from SSA. Spoofed caller-ID using random wireless and other USA subscriber numbers.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 26 Jan 21 16:05 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #4159 (new)

Date/Time: 2021-01-25 20:50 UTC
To: +12108676248
From: +12106237952
Campaign: TestCall-StaySafeStayHome

Artificial voice announces "Hello. This is just a test call. Time to stay home. Stay safe and stay home." Automated calls to wireless numbers not permitted. Caller-ID is spoofed without permission. Caller does not identify source of call or provide opt-out. High-volume campaign.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 27 Jan 21 21:41 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #4179 (new)

Date/Time: 2021-01-27 19:43 UTC

To: +13147992826

From: +13147993582

Campaign: Apple-iCloud-AccountBreached

Caller identifies themselves as calling on behalf of Apple and claims the called party's iCloud account has been breached.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 28 Jan 21 20:44 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days from now*. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #4179 (new)

Date/Time: 2021-01-27 19:43 UTC

To: +13147992826

From: +13147993582

Campaign: Apple-iCloud-AccountBreached

Caller identifies themselves as calling on behalf of Apple and claims the called party's iCloud account has been breached.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 29 Jan 21 23:17 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #4204 0 seconds ago

Campaign: Apple-iCloud-AccountBreached
Date/Time: 2021-01-29 20:50:00 +0000 UTC
To: +17736165991
From: +17736163598

Caller identifies themselves as calling on behalf of Apple and claims the called party's iCloud account has been breached.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 30 Jan 21 16:15 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #4202 0 seconds ago

Campaign: TestCall-StaySafeStayHome
Date/Time: 2021-01-29 19:19:00 +0000 UTC
To: +13163052133
From: +13164198914

Artificial voice announces "Hello. This is just a test call. Time to stay home. Stay safe and stay home." Automated calls to wireless numbers not permitted. Caller-ID is spoofed without permission. Caller does not identify source of call or provide opt-out. High-volume campaign.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 01 Feb 21 12:59 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #4207 0 seconds ago

Campaign: SSA-CalltheSSA
Date/Time: 2021-01-29 15:56:00 +0000 UTC
To: +17818882822
From: +14693000312

FRAUD. Recorded message says SSN is suspended due to law enforcement action. Caller fraudulently claims to be from SSA. Spoofed caller-ID using random wireless and other USA subscriber numbers.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 04 Feb 21 16:29 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #4223 0 seconds ago

Campaign: SSA-CalltheSSA
Date/Time: 2021-02-02 20:52:46 +0000 UTC
To: +14159335083
From: +16617772091

FRAUD. Recorded message says SSN is suspended due to law enforcement action. Caller fraudulently claims to be from SSA. Spoofed caller-ID using random wireless and other USA subscriber numbers.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 08 Feb 21 19:04 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #4261 0 seconds ago

Campaign: Apple-iCloud-AccountBreached
Date/Time: 2021-02-07 17:30:13 +0000 UTC
To: +18652069105
From: +18652062501

Caller identifies themselves as calling on behalf of Apple and claims the called party's iCloud account has been breached.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 08 Feb 21 19:06 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #4263 0 seconds ago

Campaign: Apple-iCloud-AccountBreached
Date/Time: 2021-02-06 16:23:28 +0000 UTC
To: +13609209292
From: +13609201588

Caller identifies themselves as calling on behalf of Apple and claims the called party's iCloud account has been breached.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 08 Feb 21 19:09 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #4264 0 seconds ago

Campaign: Apple-iCloud-AccountBreached
Date/Time: 2021-02-07 19:50:44 +0000 UTC
To: +18172714858
From: +18172716374

Caller identifies themselves as calling on behalf of Apple and claims the called party's iCloud account has been breached.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 22 Feb 21 16:08 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #4347 0 seconds ago

Campaign: Apple-iCloud-AccountBreached
Date/Time: 2021-02-21 17:57:30 +0000 UTC
To: +12109957090
From: +12109958183

Caller identifies themselves as calling on behalf of Apple and claims the called party's iCloud account has been breached.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 22 Feb 21 17:08 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #4349 0 seconds ago

Campaign: Apple-iCloud-AccountBreached
Date/Time: 2021-02-21 22:20:49 +0000 UTC
To: +12092511832
From: +12092515387

Caller identifies themselves as calling on behalf of Apple and claims the called party's iCloud account has been breached.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 22 Feb 21 17:38 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #4350 0 seconds ago

Campaign: Apple-iCloud-AccountBreached
Date/Time: 2021-02-21 22:14:17 +0000 UTC
To: +12092511832
From: +12092518011

Caller identifies themselves as calling on behalf of Apple and claims the called party's iCloud account has been breached.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 04 Mar 21 16:47 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #4429 0 seconds ago

Campaign: Utility-30MinDisconnect
Date/Time: 2021-03-03 18:43:48 +0000 UTC
To: +12159398987
From: +12154335463

Likely FRAUD. Recorded message says your electric service will be disconnected in 30 minutes; press 1 to make payment arrangements. Utility company is not always identified. Assorted toll-free or other numbers used as caller-ID.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 05 Mar 21 16:11 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #4456 0 seconds ago

Campaign: Discount-Avail50%
Date/Time: 2021-03-04 16:13:34 +0000 UTC
To: +17023787701
From: +18882071288

Apparent fraud. Caller offers promotions to receive a discount on the called party's voice/internet service provider bill. Automated calls to wireless numbers generally not permitted. Voice-mail message does not identify the calling entity, nor does it provide an opt-out option.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 05 Mar 21 16:55 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #4452 0 seconds ago

Campaign: CCIRR-P1FinancialImpers
Date/Time: 2021-03-04 20:53:58 +0000 UTC
To: +17862509127
From: +17865830134

Fraud. Financial institution impersonation. Caller purports to be calling from the called party's financial institution and that, based on their payment history, the recipient qualified for an interest rate reduction.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 11 Mar 21 23:16 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #4495 0 seconds ago

Campaign: Apple-iCloud-AccountBreached
Date/Time: 2021-03-10 18:34:18 +0000 UTC
To: +14782134312
From: +14782133030

Caller identifies themselves as calling on behalf of Apple and claims the called party's iCloud account has been breached.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 20 Apr 21 17:14 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #4811 0 seconds ago

Campaign: Utility-DisconnectDept
Date/Time: 2020-04-07 17:32:00 +0000 UTC
To: +17042301277
From: +12157708893

Prerecorded message claiming to be utility disconnection department and threatening power disconnection within 30 minutes due to a pending balance on the account.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 20 Apr 21 17:15 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #4812 0 seconds ago

Campaign: Utility-DisconnectDept
Date/Time: 2021-03-24 19:45:00 +0000 UTC
To: +17043235576
From: +14232051004

Prerecorded message claiming to be utility disconnection department and threatening power disconnection within 30 minutes due to a pending balance on the account.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 26 Apr 21 17:52 UTC

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

An Industry Traceback Group (ITG) participant recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin. Consistent with U.S. federal law and regulations, the ITG requests that you identify the source of this potentially fraudulent, abusive or unlawful network traffic.

To assist us in this effort, we are asking that you respond to this traceback inquiry as soon as possible, but no later than *three business days* from now. Information, including call details, related to this traceback request is available in the secure online portal linked at the end of this email.

By way of introduction, my name is Josh Bercu, and I coordinate the efforts of USTelecom's ITG, the official U.S. Federal Communications Commission (FCC)-designated registered traceback consortium that works to identify the source of illegal robocalls. In accordance with Section 13(d) of the TRACED Act, and Section 0.111(i) of the FCC's regulations, we are writing to request your assistance on a traceback investigation that we reasonably believe involves fraudulent, abusive or potentially unlawful robocalls.

My contact information is listed below, and I would be more than happy to discuss this request with you.

About the ITG and the Traceback Process

The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic and eliminate such traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see the ITG website

The ITG operates under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) under certain circumstances. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." The FCC recently clarified that voice service providers that share certain information to combat robocalls do not violate CPNI obligations under the Communications Act and its rules. See [FCC 20-96](#), ¶ 22.

The FCC's Enforcement Bureau has also concluded that "contractual provisions that prohibit, delay, or otherwise interfere with a voice service provider's cooperation with private-led traceback efforts are contrary to the spirit and goals of the TRACED Act." See [DA 20-785](#), ¶ 28. The Enforcement Bureau therefore "encourage[d] voice service providers to review their contracts and eliminate such contract provisions as soon as possible." *Id.*

Finally, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

Responding to This Request

We are asking that you submit your response to this inquiry via our secure online portal. We are asking that you submit your response to this inquiry via our secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic, and we request that you investigate that traffic and provide us with the information listed below through the portal. **For confidentiality and security purposes, provide this information *only* through the online portal. Do *not* provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network, or if one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic is able to demonstrate to you that the traffic complies with applicable U.S. laws and regulations, in the portal's comments section for the applicable traffic, identity of the end user and provide a description of the traffic and the end user's explanation of why it complies with U.S. laws and regulations.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from reaching U.S. consumers.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to call (202) 551-0761 contact ITG team via reply email should you have any questions

Best Regards,

Josh Bercu
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #4868 0 seconds ago

Campaign: SSA-Suspended
Date/Time: 2021-04-23 14:49:22 +0000 UTC
To: +15868501089
From: +15868505084

Calls fraudulently claim to be SSA threatening suspension of SSA account with immediate effect unless call-recipient presses 1 to speak to SSA legal department.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 14 May 21 14:44 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://www.ustelecom.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #4929 0 seconds ago

Campaign: SSA-P1-BenefitsCanceled (GovtImpers)

Date/Time: 2021-05-12 15:07:12 +0000 UTC

To: +17138228183

From: +17138227818

Captured recordings suggest these calls are perpetrating a SERIOUS FRAUD. Caller is impersonating a federal official. Automated message threatens that social security benefits will be canceled. Caller-ID appears to be a random toll-free number. Called party is asked to press 1 to speak to an agent. Caller-ID is random (different on each call) so blocking the ANI is not effective. This call is just one example representative of millions of similar calls. Originators please search your records for similar traffic.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 18 May 21 19:11 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://www.ustelecom.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #4952 0 seconds ago

Campaign: SSA-Suspended

Date/Time: 2021-05-17 16:14:46 +0000 UTC

To: +15754433707

From: +15754432689

Calls fraudulently claim to be SSA threatening suspension of SSA account with immediate effect unless call-recipient presses 1 to speak to SSA legal department.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 24 May 21 05:20 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://www.ustelecom.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #4972 0 seconds ago

Campaign: SSA-VT

Date/Time: 2021-05-10 17:47:00 +0000 UTC

To: +18027776961

From: +18027775361

Caller fraudulently claims to be from US Social Security Administration threatening problems with SS account. Potential TCPA violation and Vermont Consumer Protection Act violation.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 02 Jun 21 18:43 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://www.ustelecom.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #4932 0 seconds ago

Campaign: SSA-P1-BenefitsCanceled (GovtImpers)

Date/Time: 2021-05-13 19:21:09 +0000 UTC

To: +19033411326

From: +19033419889

Captured recordings suggest these calls are perpetrating a SERIOUS FRAUD. Caller is impersonating a federal official. Automated message threatens that social security benefits will be canceled. Caller-ID appears to be a random toll-free number. Called party is asked to press 1 to speak to an agent. Caller-ID is random (different on each call) so blocking the ANI is not effective. This call is just one example representative of millions of similar calls. Originators please search your records for similar traffic.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 03 Jun 21 16:47 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://www.ustelecom.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #5100 0 seconds ago

Campaign: SSA-P1-TexasFraud (GovtImpers)

Date/Time: 2021-06-02 16:50:41 +0000 UTC

To: +18126862009

From: +18125886550

FRAUD. Recorded message says SSN is suspended due to fraud in Texas or other state. Caller fraudulently claims to be from SSA. Spoofed caller-ID using random wireless and other USA subscriber numbers.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 03 Jun 21 16:50 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://www.ustelecom.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #5096 0 seconds ago

Campaign: SSA-P1-TexasFraud (GovtImpers)

Date/Time: 2021-05-10 17:14:20 +0000 UTC

To: +17026777640

From: +17026980784

FRAUD. Recorded message says SSN is suspended due to fraud in Texas or other state. Caller fraudulently claims to be from SSA. Spoofed caller-ID using random wireless and other USA subscriber numbers.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 07 Jun 21 18:24 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://www.ustelecom.org/the-industry-traceback-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #5129 0 seconds ago

Campaign: SSA-Suspended

Date/Time: 2021-06-04 17:25:49 +0000 UTC

To: +19253219905

From: +19253217087

Calls fraudulently claim to be SSA threatening suspension of SSA account with immediate effect unless call-recipient presses 1 to speak to SSA legal department.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 08 Jun 21 13:05 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://www.ustelecom.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #5143 0 seconds ago

Campaign: FedReserv-Impers
Date/Time: 2021-06-02 17:34:00 +0000 UTC
To: +14789732938
From: +14789932619

Calls claiming to be from law enforcement Federal Reserve unit where the caller alleges they found suspicious activity from their banking account which there is a legal case being filed under your name and there is an arrest warrant being issued for the same in order to talk to an officer from law enforcement unit of Federal Reserve System please press one and hold the line.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 08 Jun 21 18:38 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://www.ustelecom.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

[Redacted](#)

(URL is a private login; do not share.)

Call Details for Traceback #5158 0 seconds ago

Campaign: SSA - RegretToInform
Date/Time: 2021-06-02 15:47:00 +0000 UTC
To: +18147794654
From: +18147792409

Calls to wireless numbers. Random auto-dialing. Wireless numbers never been in service or currently not in service. Caller claims to be from Social Security Admin demanding callback prior to suspending SSN, threatening arrest. Message: "Call it from Social Security Administration we would like to notify you that we have got an order to suspend your social immediately within 24 hours due to suspicious and fraudulent activity found on your social we regret to inform you that this case is critical and time-sensitive is required your urgent attention as criminal case can be registered on your name if you do not want to get arrested press one to speak to the officer"

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 09 Jun 21 16:33 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://www.ustelecom.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #5169 0 seconds ago

Campaign: SSA-P1-BenefitsCanceled (GovtImpers)

Date/Time: 2021-06-08 18:31:00 +0000 UTC

To: +19858706025

From: +19858708308

Captured recordings suggest these calls are perpetrating a SERIOUS FRAUD. Caller is impersonating a federal official. Automated message threatens that social security benefits will be canceled. Caller-ID appears to be a random toll-free number. Called party is asked to press 1 to speak to an agent. Caller-ID is random (different on each call) so blocking the ANI is not effective. This call is just one example representative of millions of similar calls. Originators please search your records for similar traffic.

From: traceback-notice@tracebacks.org
To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com
Date: 23 Jun 21 21:53 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://www.ustelecom.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #5330 0 seconds ago

Campaign: SSA-CrimeInvestigation
Date/Time: 2021-06-22 18:44:00 +0000 UTC
To: +19707780256
From: +19787613984

Caller is impersonating a federal official. Automated voice claims suspicious activity on your social security number. "Hello this is an urgent notice enforcement agencies to suspend your social security number on an immediate basis and money-laundering case so I want you to reach us immediately your Banking and government services are blocked now due to suspension of your Social Security number to know more about this case File reaches back on same number before we issue an arrest warrant for Crime investigation if we do not hear back from you will be considered as an intentional crime"

From: traceback-notice@tracebacks.org
To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com
Date: 26 Jul 21 18:48 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://www.ustelecom.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #5526 0 seconds ago

Campaign: Amazon - Acct On Hold
Date/Time: 2021-07-15 16:45:00 +0000 UTC
To: +17089275564
From: +17089273851

Automated voice claiming to be Amazon customer service calling about a recent order and due to suspicious activity the account may be placed on hold. Wireless numbers never been in service or currently not in service.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 26 Jul 21 18:51 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://www.ustelecom.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #5585 0 seconds ago

Campaign: SSA-KindlyPressOne

Date/Time: 2021-07-23 22:23:34 +0000 UTC

To: +12088903944

From: +12088643308

These calls fraudulently claim to be from the SSA and advise a legal enforcement action has been filed on social security number.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 05 Aug 21 23:00 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://www.ustelecom.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #5693 0 seconds ago

Campaign: Amazon-SuspiciousCharge

Date/Time: 2021-08-04 00:07:00 +0000 UTC

To: +15705743191

From: +15705747280

Calls to wireless numbers impersonating Amazon, claiming suspicious charges on customer's account. Random auto-dialing. Wireless numbers never been in service or currently not in service.

From: traceback-notice@tracebacks.org
To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com
Date: 14 Sep 21 14:18 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://www.ustelecom.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #6048 0 seconds ago

Campaign: Legal Enforcement Notice
Date/Time: 2021-09-13 16:46:15 +0000 UTC
To: +19048816709
From: +19706477298

Pre-recorded calls from spoofed numbers to consumers stating a warrant has been issued against them due to fraudulent activity and to press 1 for more information.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 08 Oct 21 13:52 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://www.ustelecom.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #6391 0 seconds ago

Campaign: Amazon-AuthorizeOrder

Date/Time: 2021-10-07 20:54:33 +0000 UTC

To: +17276446307

From: +17273004930

Calls to wireless numbers impersonating Amazon, calling to authorize an order that was placed.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 19 Oct 21 17:37 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://www.ustelecom.org/the-industry-traceback-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #6525 0 seconds ago

Campaign: SSA-KindlyPressOne

Date/Time: 2021-10-18 21:23:19 +0000 UTC

To: +17025610226

From: +19047855234

These calls fraudulently claim to be from the SSA and advise a legal enforcement action has been filed on social security number.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 21 Oct 21 17:33 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://www.ustelecom.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #6591 0 seconds ago

Campaign: SSA-P1-TexasFraud (GovtImpers)

Date/Time: 2021-10-20 19:29:52 +0000 UTC

To: +18605181089

From: +13173394249

FRAUD. Recorded message says SSN is suspended due to fraud in Texas or other state. Caller fraudulently claims to be from SSA. Spoofed caller-ID using random wireless and other USA subscriber numbers.

From: traceback-notice@tracebacks.org
To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com
Date: 21 Oct 21 18:59 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://www.ustelecom.org/the-industry-traceback-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #6593 0 seconds ago

Campaign: SSA-P1-TexasFraud (GovtImpers)
Date/Time: 2021-10-20 18:17:52 +0000 UTC
To: +18303253492
From: +13175941323

FRAUD. Recorded message says SSN is suspended due to fraud in Texas or other state. Caller fraudulently claims to be from SSA. Spoofed caller-ID using random wireless and other USA subscriber numbers.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 22 Oct 21 13:41 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://www.ustelecom.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #6598 0 seconds ago

Campaign: Utility-30MinDisconnect

Date/Time: 2021-10-21 18:23:49 +0000 UTC

To: +19165216493

From: +19165214366

Likely FRAUD. Recorded message says your electric service will be disconnected in 30 minutes; press 1 to make payment arrangements. Utility company is not always identified. Assorted toll-free or other numbers used as caller-ID.

From: traceback-notice@tracebacks.org
To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com
Date: 29 Oct 21 20:44 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://www.ustelecom.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #6738 0 seconds ago

Campaign: SSA-P1-TexasFraud (GovtImpers)
Date/Time: 2021-10-27 15:56:52 +0000 UTC
To: +16625822679
From: +16625843805

FRAUD. Recorded message says SSN is suspended due to fraud in Texas or other state. Caller fraudulently claims to be from SSA. Spoofed caller-ID using random wireless and other USA subscriber numbers.

From: traceback-notice@tracebacks.org
To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com
Date: 01 Nov 21 13:33 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://www.ustelecom.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #6737 0 seconds ago

Campaign: SSA-P1-TexasFraud (GovtImpers)
Date/Time: 2021-10-27 16:07:18 +0000 UTC
To: +15025231025
From: +15025299770

FRAUD. Recorded message says SSN is suspended due to fraud in Texas or other state. Caller fraudulently claims to be from SSA. Spoofed caller-ID using random wireless and other USA subscriber numbers.

From: traceback-notice@tracebacks.org
To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com
Date: 01 Nov 21 14:50 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://www.ustelecom.org/the-industry-traceback-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #6736 0 seconds ago

Campaign: SSA-P1-TexasFraud (GovtImpers)
Date/Time: 2021-10-27 18:25:09 +0000 UTC
To: +15025231025
From: +15025256377

FRAUD. Recorded message says SSN is suspended due to fraud in Texas or other state. Caller fraudulently claims to be from SSA. Spoofed caller-ID using random wireless and other USA subscriber numbers.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 05 Nov 21 15:23 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://www.ustelecom.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #6833 0 seconds ago

Campaign: SSA-P1-TexasFraud (GovtImpers)

Date/Time: 2021-11-03 16:40:00 +0000 UTC

To: +18162107256

From: +18162156809

FRAUD. Recorded message says SSN is suspended due to fraud in Texas or other state. Caller fraudulently claims to be from SSA. Spoofed caller-ID using random wireless and other USA subscriber numbers.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 05 Nov 21 15:31 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://www.ustelecom.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #6824 0 seconds ago

Campaign: SSA-P1-TexasFraud (GovtImpers)

Date/Time: 2021-11-03 15:15:03 +0000 UTC

To: +13107467544

From: +13107494372

FRAUD. Recorded message says SSN is suspended due to fraud in Texas or other state. Caller fraudulently claims to be from SSA. Spoofed caller-ID using random wireless and other USA subscriber numbers.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 08 Nov 21 20:15 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://www.ustelecom.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #6882 0 seconds ago

Campaign: Hotel-ComplimentaryStay

Date/Time: 2021-11-05 01:29:00 +0000 UTC

To: +18306370945

From: +18062276904

Hotel impersonation offering a complimentary stay. Calls to wireless numbers. Random auto-dialing. Wireless numbers never been in service or currently not in service.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 08 Nov 21 20:33 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://www.ustelecom.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #6885 0 seconds ago

Campaign: Hotel-ComplimentaryStay

Date/Time: 2021-11-03 19:58:00 +0000 UTC

To: +14347701779

From: +17572013137

Hotel impersonation offering a complimentary stay. Calls to wireless numbers. Random auto-dialing. Wireless numbers never been in service or currently not in service.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 08 Nov 21 21:55 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://www.ustelecom.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #6886 0 seconds ago

Campaign: Hotel-ComplimentaryStay

Date/Time: 2021-11-03 19:35:00 +0000 UTC

To: +14252476290

From: +14254307302

Hotel impersonation offering a complimentary stay. Calls to wireless numbers. Random auto-dialing. Wireless numbers never been in service or currently not in service.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 09 Nov 21 18:52 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://www.ustelecom.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #6884 0 seconds ago

Campaign: Hotel-ComplimentaryStay

Date/Time: 2021-11-04 00:44:00 +0000 UTC

To: +15012701303

From: +18706805335

Hotel impersonation offering a complimentary stay. Calls to wireless numbers. Random auto-dialing. Wireless numbers never been in service or currently not in service.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 22 Nov 21 19:02 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://www.ustelecom.org/the-industry-traceback-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #7044 0 seconds ago

Campaign: Amazon-AuthorizeOrder

Date/Time: 2021-11-16 16:33:07 +0000 UTC

To: +18023538170

From: +18016797189

Calls to wireless numbers impersonating Amazon, calling to authorize an order that was placed.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 08 Dec 21 14:25 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://www.ustelecom.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #7249 0 seconds ago

Campaign: SSA-KindlyPressOne

Date/Time: 2021-12-07 16:26:43 +0000 UTC

To: +15129929046

From: +15129922595

These calls fraudulently claim to be from the SSA and advise a legal enforcement action has been filed on social security number.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 08 Dec 21 15:02 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://www.ustelecom.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #7250 0 seconds ago

Campaign: SSA-KindlyPressOne

Date/Time: 2021-12-06 13:46:31 +0000 UTC

To: +15129929046

From: +15129921339

These calls fraudulently claim to be from the SSA and advise a legal enforcement action has been filed on social security number.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 13 Jan 22 17:40 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://www.ustelecom.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #7633 0 seconds ago

Campaign: LegalDept-Action-P1

Date/Time: 2022-01-12 21:52:49 +0000 UTC

To: +12256509409

From: +12256503614

Calls claiming to be from the Legal Department, advising about the recipient's case and how legal action will be taken against them. To speak to a federal agent they need to press one.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 14 Jan 22 23:49 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://www.ustelecom.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #7655 0 seconds ago

Campaign: SSA-KindlyPressOne-2
Date/Time: 2022-01-10 16:20:00 +0000 UTC
To: +17178440299
From: +18709003693

These calls fraudulently claim to be from the SSA and advise a legal enforcement action has been filed on social security number.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com

Date: 10 Feb 22 20:58 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #8047 0 seconds ago

Campaign: Amazon-SuspiciousCharge

Date/Time: 2022-02-08 22:56:32 +0000 UTC

To: +18642001971

From: +18642009362

Calls to wireless numbers impersonating Amazon, claiming suspicious charges on customer's account. Random auto-dialing. Wireless numbers never been in service or currently not in service.

From: traceback-notice@tracebacks.org
To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com
Date: 10 Feb 22 21:00 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:
[Redacted](#)
(URL is a private login; do not share.)

Call Details for Traceback #8048 0 seconds ago

Campaign: Amazon-SuspiciousCharge
Date/Time: 2022-02-08 19:04:06 +0000 UTC
To: +13045905202
From: +13045904780

Calls to wireless numbers impersonating Amazon, claiming suspicious charges on customer's account. Random auto-dialing. Wireless numbers never been in service or currently not in service.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 10 Feb 22 22:31 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #8050 0 seconds ago

Campaign: Amazon-SuspiciousCharge

Date/Time: 2022-02-08 18:20:12 +0000 UTC

To: +12012505192

From: +12012508878

Calls to wireless numbers impersonating Amazon, claiming suspicious charges on customer's account. Random auto-dialing. Wireless numbers never been in service or currently not in service.

From: traceback-notice@tracebacks.org
To: katherine.rosales@smartbiztel.com
Date: 01 Mar 22 09:30 UTC

INDUSTRY TRACEBACK GROUP

Monthly Metrics - **Smartbiz Telecom, LLC**

noc, you can find your organization's **Monthly Metrics** below.

Your Summary:

Total Hops	Open	POE	Downstream	Orig	No Resp	Not Found	Avg Response	Campaigns
3	0	0	0	0	0	0	1 hour 9 minutes	1

Upstream Summary:

Provider	Total Hops	Open	POE	Orig	No Resp	Not Found
Opextel, LLC	3	0	0	0	0	0

If you have any trouble seeing this email, please visit:

[https://portal.tracebacks.org/email-redirect?](https://portal.tracebacks.org/email-redirect?location=/providers/provider/summaries/386&token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImthdGhlcmluZS5yb3NhbGVzQHNTYXJ0Yml6dGVsLmNvbSIsImklIjoxMDAzMCwianRpIjojMTAwMzAifQ.mgP_5jeEKGcuVOKrFTc0xCGi80wMxdTcV14mBQnyu)

[location=/providers/provider/summaries/386&token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImthdGhlcmluZS5yb3NhbGVzQHNTYXJ0Yml6dGVsLmNvbSIsImklIjoxMDAzMCwianRpIjojMTAwMzAifQ.mgP_5jeEKGcuVOKrFTc0xCGi80wMxdTcV14mBQnyu](https://portal.tracebacks.org/email-redirect?location=/providers/provider/summaries/386&token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImthdGhlcmluZS5yb3NhbGVzQHNTYXJ0Yml6dGVsLmNvbSIsImklIjoxMDAzMCwianRpIjojMTAwMzAifQ.mgP_5jeEKGcuVOKrFTc0xCGi80wMxdTcV14mBQnyu)
rg

From: traceback-notice@tracebacks.org
To: eborrero@smartbiztel.com
Date: 01 Mar 22 09:30 UTC

INDUSTRY TRACEBACK GROUP

Monthly Metrics - Smartbiz Telecom, LLC

Eduardo Borrero, you can find your organization's Monthly Metrics below.

Your Summary:

Total Hops	Open	POE	Downstream	Orig	No Resp	Not Found	Avg Response	Campaigns
3	0	0	0	0	0	0	1 hour 9 minutes	1

Upstream Summary:

Provider	Total Hops	Open	POE	Orig	No Resp	Not Found
Opextel, LLC	3	0	0	0	0	0

If you have any trouble seeing this email, please visit:
[https://portal.tracebacks.org/email-redirect?](https://portal.tracebacks.org/email-redirect?location=/providers/provider/summaries/386&token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybWVib3JyZXJvQHNtYXJ0Yml6dGVsLmNvbSIsImklIjoxMTIwMSwianRpIjoimTEyMDEifQ.mLIJeQG-KjgTTQjSIFBnwiLKZjvZ2heqjiR9VQJGQEk)

[location=/providers/provider/summaries/386&token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybWVib3JyZXJvQHNtYXJ0Yml6dGVsLmNvbSIsImklIjoxMTIwMSwianRpIjoimTEyMDEifQ.mLIJeQG-KjgTTQjSIFBnwiLKZjvZ2heqjiR9VQJGQEk](https://portal.tracebacks.org/email-redirect?location=/providers/provider/summaries/386&token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybWVib3JyZXJvQHNtYXJ0Yml6dGVsLmNvbSIsImklIjoxMTIwMSwianRpIjoimTEyMDEifQ.mLIJeQG-KjgTTQjSIFBnwiLKZjvZ2heqjiR9VQJGQEk)

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com

Date: 01 Mar 22 09:30 UTC

INDUSTRY TRACEBACK GROUP

Monthly Metrics - **Smartbiz Telecom, LLC**

NOC, you can find your organization's **Monthly Metrics** below.

Your Summary:

Total Hops	Open	POE	Downstream	Orig	No Resp	Not Found	Avg Response	Campaigns
3	0	0	0	0	0	0	1 hour 9 minutes	1

Upstream Summary:

Provider	Total Hops	Open	POE	Orig	No Resp	Not Found
Opextel, LLC	3	0	0	0	0	0

If you have any trouble seeing this email, please visit:

[https://portal.tracebacks.org/email-redirect?](https://portal.tracebacks.org/email-redirect?location=/providers/provider/summaries/386&token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6Im5vY0BzbWYdGJpenRlbC5jb20iLCJpZCI6NjQ4LCJqdGkiOiI2NDgifQ.ncWchlTO9C2yPyehwcznh_cX9BRzWVdalD83bJzqYBE)

[location=/providers/provider/summaries/386&token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6Im5vY0BzbWYdGJpenRlbC5jb20iLCJpZCI6NjQ4LCJqdGkiOiI2NDgifQ.ncWchlTO9C2yPyehwcznh_cX9BRzWVdalD83bJzqYBE](https://portal.tracebacks.org/email-redirect?location=/providers/provider/summaries/386&token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6Im5vY0BzbWYdGJpenRlbC5jb20iLCJpZCI6NjQ4LCJqdGkiOiI2NDgifQ.ncWchlTO9C2yPyehwcznh_cX9BRzWVdalD83bJzqYBE)

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 07 Mar 22 21:49 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #8319 0 seconds ago

Campaign: Travel Scam-Costco
Date/Time: 2022-03-04 23:47:32 +0000 UTC
To: +19282714872
From: +16027240592

Recorded voice offering hospitality incentive through high-volume calling campaign, including to wireless numbers. Use of brand names, including Costco, apparently fraudulently without permission. Caller also falsely claims association with Hilton and Marriott. Suspected caller-ID spoofing due to high volume of originating numbers. Failure to identify the entity responsible for the call.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 08 Mar 22 02:34 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #8311 0 seconds ago

Campaign: Amazon-AuthorizeOrder

Date/Time: 2022-03-06 16:11:10 +0000 UTC

To: +16054001440

From: +16059898493

Calls to wireless numbers impersonating Amazon, calling to authorize an order that was placed.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 09 Mar 22 15:57 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #8343 0 seconds ago

Campaign: Utility-ElectricRebateCheck-P1

Date/Time: 2022-03-08 18:33:18 +0000 UTC

To: +16143273052

From: +16143543412

Recorded message says you will receive a rebate check for utility service due to an overcharge by a third party supplier. Assorted toll-free or other numbers used as caller-ID.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 09 Mar 22 17:20 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #8338 0 seconds ago

Campaign: Utility-ElectricRebateCheck-P1

Date/Time: 2022-03-08 16:01:25 +0000 UTC

To: +12162581980

From: +12162058776

Recorded message says you will receive a rebate check for utility service due to an overcharge by a third party supplier. Assorted toll-free or other numbers used as caller-ID.

From: traceback-notice@tracebacks.org
To: eborrero@smartbiztel.com
Date: 01 Apr 22 09:30 UTC

INDUSTRY TRACEBACK GROUP

Monthly Metrics - Smartbiz Telecom, LLC

Eduardo Borrero, you can find your organization's Monthly Metrics below.

Your Summary:

Total Hops	Open	POE	Downstream	Orig	No Resp	Not Found	Avg Response	Campaigns
3	0	0	0	0	0	0	3 hours 20 minutes	2

Upstream Summary:

Provider	Total Hops	Open	POE	Orig	No Resp	Not Found
Lata 1 Communications Inc.	1	0	1	0	0	0
Telconus / Telcon US / Telcon Voice / Whisl	3	0	0	0	0	0

If you have any trouble seeing this email, please visit:
[https://portal.tracebacks.org/email-redirect?](https://portal.tracebacks.org/email-redirect?location=/providers/provider/summaries/386&token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImVib3JyZXJvQHNtYXJ0Yml6dGVsLmNvbSIsImlkIjoxMTIwMSwianRpIjoiTTEyMTEyMDEifQ.mLIJeQG-KjgTTQjSIFBnwiLKZjvZ2heqjiR9VQJGQEk)

[location=/providers/provider/summaries/386&token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImVib3JyZXJvQHNtYXJ0Yml6dGVsLmNvbSIsImlkIjoxMTIwMSwianRpIjoiTTEyMTEyMDEifQ.mLIJeQG-KjgTTQjSIFBnwiLKZjvZ2heqjiR9VQJGQEk](https://portal.tracebacks.org/email-redirect?location=/providers/provider/summaries/386&token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImVib3JyZXJvQHNtYXJ0Yml6dGVsLmNvbSIsImlkIjoxMTIwMSwianRpIjoiTTEyMTEyMDEifQ.mLIJeQG-KjgTTQjSIFBnwiLKZjvZ2heqjiR9VQJGQEk)

From: traceback-notice@tracebacks.org
To: katherine.rosales@smartbiztel.com
Date: 01 Apr 22 09:30 UTC

INDUSTRY TRACEBACK GROUP

Monthly Metrics - Smartbiz Telecom, LLC

noc, you can find your organization's Monthly Metrics below.

Your Summary:

Total Hops	Open	POE	Downstream	Orig	No Resp	Not Found	Avg Response	Campaigns
3	0	0	0	0	0	0	3 hours 20 minutes	2

Upstream Summary:

Provider	Total Hops	Open	POE	Orig	No Resp	Not Found
Lata 1 Communications Inc.	1	0	1	0	0	0
Telconus / Telcon US / Telcon Voice / Whisl	3	0	0	0	0	0

If you have any trouble seeing this email, please visit:
[https://portal.tracebacks.org/email-redirect?](https://portal.tracebacks.org/email-redirect?location=/providers/provider/summaries/386&token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImthdGhlcmluZS5yb3NhbGVzQHNtYXJ0Yml6dGVsLmNvbSIsImklIjoxMDAzMCwianRpIjojMTAwMzAifQ.mgP_5jeEKGCUVOKrFTc0xCGi80wMxdTcV14mBQnyu)

[location=/providers/provider/summaries/386&token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImthdGhlcmluZS5yb3NhbGVzQHNtYXJ0Yml6dGVsLmNvbSIsImklIjoxMDAzMCwianRpIjojMTAwMzAifQ.mgP_5jeEKGCUVOKrFTc0xCGi80wMxdTcV14mBQnyu](https://portal.tracebacks.org/email-redirect?location=/providers/provider/summaries/386&token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImthdGhlcmluZS5yb3NhbGVzQHNtYXJ0Yml6dGVsLmNvbSIsImklIjoxMDAzMCwianRpIjojMTAwMzAifQ.mgP_5jeEKGCUVOKrFTc0xCGi80wMxdTcV14mBQnyu)
rg

From: traceback-notice@tracebacks.org
To: noc@smartbiztel.com
Date: 01 Apr 22 09:30 UTC

INDUSTRY TRACEBACK GROUP

Monthly Metrics - Smartbiz Telecom, LLC

NOC, you can find your organization's Monthly Metrics below.

Your Summary:

Total Hops	Open	POE	Downstream	Orig	No Resp	Not Found	Avg Response	Campaigns
3	0	0	0	0	0	0	3 hours 20 minutes	2

Upstream Summary:

Provider	Total Hops	Open	POE	Orig	No Resp	Not Found
Lata 1 Communications Inc.	1	0	1	0	0	0
Telconus / Telcon US / Telcon Voice / Whisl	3	0	0	0	0	0

If you have any trouble seeing this email, please visit:
[https://portal.tracebacks.org/email-redirect?](https://portal.tracebacks.org/email-redirect?location=/providers/provider/summaries/386&token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6Im5vY0BzbWVydGJpenRlbC5jb20iLCJpZCI6NjQ4LCJqdGkiOiI2NDgifQ.ncWchlTO9C2yPyehwcznh_cX9BRzWVdalD83bJzqYBE)

[location=/providers/provider/summaries/386&token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6Im5vY0BzbWVydGJpenRlbC5jb20iLCJpZCI6NjQ4LCJqdGkiOiI2NDgifQ.ncWchlTO9C2yPyehwcznh_cX9BRzWVdalD83bJzqYBE](https://portal.tracebacks.org/email-redirect?location=/providers/provider/summaries/386&token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6Im5vY0BzbWVydGJpenRlbC5jb20iLCJpZCI6NjQ4LCJqdGkiOiI2NDgifQ.ncWchlTO9C2yPyehwcznh_cX9BRzWVdalD83bJzqYBE)

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 01 Apr 22 17:26 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #8606 0 seconds ago

Campaign: Amazon-AuthorizeOrder-P3

Date/Time: 2022-03-30 21:26:27 +0000 UTC

To: +18649347810

From: +12073648869

Calls to wireless numbers impersonating Amazon, calling to authorize an order that was placed.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 13 Apr 22 14:20 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #8718 0 seconds ago

Campaign: Hotel-ComplimentaryStay

Date/Time: 2022-04-08 01:20:28 +0000 UTC

To: +15756187233

From: +15758883317

Hotel impersonation offering a complimentary stay. Calls to wireless numbers. Random auto-dialing. Wireless numbers never been in service or currently not in service.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 13 Apr 22 15:45 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #8719 0 seconds ago

Campaign: Hotel-ComplimentaryStay

Date/Time: 2022-04-11 22:04:26 +0000 UTC

To: +19712842814

From: +19715125516

Hotel impersonation offering a complimentary stay. Calls to wireless numbers. Random auto-dialing. Wireless numbers never been in service or currently not in service.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 13 Apr 22 15:46 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #8715 0 seconds ago

Campaign: Hotel-ComplimentaryStay

Date/Time: 2022-04-09 00:39:50 +0000 UTC

To: +15302405109

From: +15308172249

Hotel impersonation offering a complimentary stay. Calls to wireless numbers. Random auto-dialing. Wireless numbers never been in service or currently not in service.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 13 Apr 22 15:47 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #8721 0 seconds ago

Campaign: Hotel-ComplimentaryStay

Date/Time: 2022-04-11 19:00:32 +0000 UTC

To: +16052229305

From: +16059494317

Hotel impersonation offering a complimentary stay. Calls to wireless numbers. Random auto-dialing. Wireless numbers never been in service or currently not in service.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 13 Apr 22 18:28 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #8736 0 seconds ago

Campaign: Apple-SuspiciousActivity

Date/Time: 2022-04-01 16:35:00 +0000 UTC

To: +12062327528

From: +12062322521

Caller claiming to be from Apple Security regarding suspicious activity on a cloud account.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 14 Apr 22 14:54 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #8737 0 seconds ago

Campaign: StudentLoan-Forgiveness

Date/Time: 2022-04-05 20:24:00 +0000 UTC

To: +13194313880

From: +15416558857

Calls to recipients offering student loan forgiveness. Recipients may not have student loans.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 14 Apr 22 14:56 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #8739 0 seconds ago

Campaign: ImproperTN-Use
Date/Time: 2022-03-30 16:01:00 +0000 UTC
To: +17023375905
From: +12012000012

Improper use of number on authenticated call as part of bulk calling campaign.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 14 Apr 22 14:58 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #8741 0 seconds ago

Campaign: ImproperTN-Use
Date/Time: 2022-03-30 16:08:00 +0000 UTC
To: +17025262784
From: +12012000012

Improper use of number on authenticated call as part of bulk calling campaign.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 14 Apr 22 15:00 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #8742 0 seconds ago

Campaign: ImproperTN-Use
Date/Time: 2022-03-30 16:02:00 +0000 UTC
To: +17752300611
From: +12012000012

Improper use of number on authenticated call as part of bulk calling campaign.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 22 Apr 22 21:01 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #8840 0 seconds ago

Campaign: Travel-Brand-Impers
Date/Time: 2022-04-21 18:51:43 +0000 UTC
To: +17039990645
From: +17032132856

Recorded voice offering hospitality incentive through high-volume calling campaign, including to wireless numbers. Confirmed fraudulent use of third-party brand names, including Marriott, without permission of the brand owner. Caller also falsely claims association with Hilton and Four Seasons. Suspected caller-ID spoofing due to high volume of originating numbers. Failure to identify the entity responsible for the call.

From: traceback-notice@tracebacks.org
To: noc@smartbiztel.com
Date: 01 May 22 09:30 UTC

INDUSTRY TRACEBACK GROUP

Monthly Metrics - Smartbiz Telecom, LLC

NOC, you can find your organization's traceback-related metrics for the last 30 days below.

Your Summary:

Total Hops	Open	POE	Downstream	Orig	No Resp	Not Found	Avg Response	Campaigns
8	0	0	0	0	0	0	49 minutes 13 seconds	3

Upstream Summary:

Provider	Total Hops	Open	POE	Orig	No Resp	Not Found
Lata 1 Communications Inc.	4	0	4	0	0	0
Etelix.com USA, LLC	1	0	1	0	0	0
Telconus / Telcon US / Telcon Voice / Whisl	6	0	0	0	0	0

If you have any trouble seeing this email, please visit:
[https://portal.tracebacks.org/email-redirect?](https://portal.tracebacks.org/email-redirect?location=/providers/provider/summaries/386&token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6Im5vY0BzbWYdGJpenRlbC5jb20iLCJpZCI6NjQ4LCJqdGkiOiI2NDgifQ.ncWchlTO9C2yPyehwcznh_cX9BRzWVdaID83bJzqYBE)

[location=/providers/provider/summaries/386&token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6Im5vY0BzbWYdGJpenRlbC5jb20iLCJpZCI6NjQ4LCJqdGkiOiI2NDgifQ.ncWchlTO9C2yPyehwcznh_cX9BRzWVdaID83bJzqYBE](https://portal.tracebacks.org/email-redirect?location=/providers/provider/summaries/386&token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6Im5vY0BzbWYdGJpenRlbC5jb20iLCJpZCI6NjQ4LCJqdGkiOiI2NDgifQ.ncWchlTO9C2yPyehwcznh_cX9BRzWVdaID83bJzqYBE)

From: traceback-notice@tracebacks.org
To: katherine.rosales@smartbiztel.com
Date: 01 May 22 09:30 UTC

INDUSTRY TRACEBACK GROUP

Monthly Metrics - Smartbiz Telecom, LLC

noc, you can find your organization's traceback-related metrics for the last 30 days below.

Your Summary:

Total Hops	Open	POE	Downstream	Orig	No Resp	Not Found	Avg Response	Campaigns
8	0	0	0	0	0	0	49 minutes 13 seconds	3

Upstream Summary:

Provider	Total Hops	Open	POE	Orig	No Resp	Not Found
Lata 1 Communications Inc.	4	0	4	0	0	0
Etelix.com USA, LLC	1	0	1	0	0	0
Telconus / Telcon US / Telcon Voice / Whisl	6	0	0	0	0	0

If you have any trouble seeing this email, please visit:
[https://portal.tracebacks.org/email-redirect?](https://portal.tracebacks.org/email-redirect?location=/providers/provider/summaries/386&token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImthdGhlcmluZS5yb3NhbgVzQHNTYXJ0Yml6dGVsLmNvbSIsImkiOiJoxMDAzMCwianRpIjoMTAwMzAifQ.mgP_5jeEKGcuVOKrFTc0xCGi80wMxdTcV14mBQnyurg)

[location=/providers/provider/summaries/386&token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImthdGhlcmluZS5yb3NhbgVzQHNTYXJ0Yml6dGVsLmNvbSIsImkiOiJoxMDAzMCwianRpIjoMTAwMzAifQ.mgP_5jeEKGcuVOKrFTc0xCGi80wMxdTcV14mBQnyurg](https://portal.tracebacks.org/email-redirect?location=/providers/provider/summaries/386&token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImthdGhlcmluZS5yb3NhbgVzQHNTYXJ0Yml6dGVsLmNvbSIsImkiOiJoxMDAzMCwianRpIjoMTAwMzAifQ.mgP_5jeEKGcuVOKrFTc0xCGi80wMxdTcV14mBQnyurg)

From: traceback-notice@tracebacks.org
To: eborrero@smartbiztel.com
Date: 01 May 22 09:30 UTC

INDUSTRY TRACEBACK GROUP

Monthly Metrics - Smartbiz Telecom, LLC

Eduardo Borrero, you can find your organization's traceback-related metrics for the last 30 days below.

Your Summary:

Total Hops	Open	POE	Downstream	Orig	No Resp	Not Found	Avg Response	Campaigns
8	0	0	0	0	0	0	49 minutes 13 seconds	3

Upstream Summary:

Provider	Total Hops	Open	POE	Orig	No Resp	Not Found
Lata 1 Communications Inc.	4	0	4	0	0	0
Etelix.com USA, LLC	1	0	1	0	0	0
Telconus / Telcon US / Telcon Voice / Whisl	6	0	0	0	0	0

If you have any trouble seeing this email, please visit:
[https://portal.tracebacks.org/email-redirect?](https://portal.tracebacks.org/email-redirect?location=/providers/provider/summaries/386&token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImVib3JyZXJvQHNtYXJ0YmI6dGVsLmNvbSIsImklIjoxMTIwMSwianRpIjoieMTEyMDEifQ.mLIJeQG-KjgTTQjSIFBnwiLKZjvZ2heqjiR9VQJGQEk)

[location=/providers/provider/summaries/386&token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImVib3JyZXJvQHNtYXJ0YmI6dGVsLmNvbSIsImklIjoxMTIwMSwianRpIjoieMTEyMDEifQ.mLIJeQG-KjgTTQjSIFBnwiLKZjvZ2heqjiR9VQJGQEk](https://portal.tracebacks.org/email-redirect?location=/providers/provider/summaries/386&token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImVib3JyZXJvQHNtYXJ0YmI6dGVsLmNvbSIsImklIjoxMTIwMSwianRpIjoieMTEyMDEifQ.mLIJeQG-KjgTTQjSIFBnwiLKZjvZ2heqjiR9VQJGQEk)

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 02 May 22 20:56 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #8885 0 seconds ago

Campaign: AutoWarranty-Expiring

Date/Time: 2022-04-26 18:12:00 +0000 UTC

To: +14086302511

From: +14086304545

Significant amount of spoofed calls per day using a prerecorded message suggesting car warranty is expiring. Likely no consent to make calls.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 19 May 22 18:42 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #9127 0 seconds ago

Campaign: StudentLoan-ForgivenessCenter

Date/Time: 2022-05-17 20:30:22 +0000 UTC

To: +12069725785

From: +18307234696

Call to mobile using pre-recorded voice. Referencing student loan Forgiveness center; Some call recipients do not have student loans.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 26 May 22 00:50 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #9194 0 seconds ago

Campaign: Bank-Impers-P2
Date/Time: 2022-05-19 01:35:00 +0000 UTC
To: +15088132683
From: +18004321000

Bank of America Impersonation. Client receives a call from a spoofed number claiming to be a Bank of America representative. The caller attempts to social engineer victim into providing sensitive information and executing transactions.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 26 May 22 15:29 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #9197 0 seconds ago

Campaign: Bank-Impers-P2
Date/Time: 2022-05-16 23:40:00 +0000 UTC
To: +14095494262
From: +18004321000

Bank of America Impersonation. Client receives a call from a spoofed number claiming to be a Bank of America representative. The caller attempts to social engineer victim into providing sensitive information and executing transactions.

From: traceback-notice@tracebacks.org
To: katherine.rosales@smartbiztel.com
Date: 01 Jun 22 09:30 UTC

INDUSTRY TRACEBACK GROUP

Monthly Metrics - **Smartbiz Telecom, LLC**

noc, you can find your organization's traceback-related metrics for the last 30 days below.

Your Summary:

Total Hops	Open	POE	Downstream	Orig	No Resp	Not Found	Avg Response	Campaigns
2	0	0	0	0	0	0	3 hours 38 minutes	2

Upstream Summary:

Provider	Total Hops	Open	POE	Orig	No Resp	Not Found
Telconus / Telcon US / Telcon Voice / Whisl	4	0	0	0	0	0

If you have any trouble seeing this email, please visit:
<https://portal.tracebacks.org/email-redirect?location=/providers/provider/summaries/386&userId=10030&token=fd59d524-dea4-4787-a4d7-f10bba1d50a7>

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com

Date: 01 Jun 22 09:30 UTC

INDUSTRY TRACEBACK GROUP

Monthly Metrics - **Smartbiz Telecom, LLC**

NOC, you can find your organization's traceback-related metrics for the last 30 days below.

Your Summary:

Total Hops	Open	POE	Downstream	Orig	No Resp	Not Found	Avg Response	Campaigns
2	0	0	0	0	0	0	3 hours 38 minutes	2

Upstream Summary:

Provider	Total Hops	Open	POE	Orig	No Resp	Not Found
Telconus / Telcon US / Telcon Voice / Whisl	4	0	0	0	0	0

If you have any trouble seeing this email, please visit:
<https://portal.tracebacks.org/email-redirect?location=/providers/provider/summaries/386&userId=648&token=7097d9c6-08cd-4309-9f6d-8256b74987a6>

From: traceback-notice@tracebacks.org

To: eborrero@smartbiztel.com

Date: 01 Jun 22 09:30 UTC

INDUSTRY TRACEBACK GROUP

Monthly Metrics - **Smartbiz Telecom, LLC**

Eduardo Borrero, you can find your organization's traceback-related metrics for the last 30 days below.

Your Summary:

Total Hops	Open	POE	Downstream	Orig	No Resp	Not Found	Avg Response	Campaigns
2	0	0	0	0	0	0	3 hours 38 minutes	2

Upstream Summary:

Provider	Total Hops	Open	POE	Orig	No Resp	Not Found
Telconus / Telcon US / Telcon Voice / Whisl	4	0	0	0	0	0

If you have any trouble seeing this email, please visit:

<https://portal.tracebacks.org/email-redirect?location=/providers/provider/summaries/386&userId=11201&token=d8d15751-2140-48e9-9eff-8ac43509989c>

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 02 Jun 22 20:11 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #9227 0 seconds ago

Campaign: SpamCalls-Spoofed-P1

Date/Time: 2022-05-26 17:08:00 +0000 UTC

To: +17245967319

From: +17246230023

Spoofed calls impersonating local businesses and government officials causing disruption.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 13 Jun 22 12:57 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #9275 0 seconds ago

Campaign: Hotel-ComplimentaryStay

Date/Time: 2022-06-08 17:51:09 +0000 UTC

To: +17203152669

From: +13033370870

Hotel impersonation offering a complimentary stay. Calls to wireless numbers. Random auto-dialing. Wireless numbers never been in service or currently not in service.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 13 Jun 22 13:01 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #9272 0 seconds ago

Campaign: Hotel-ComplimentaryStay

Date/Time: 2022-06-07 20:21:17 +0000 UTC

To: +14437210768

From: +14104516636

Hotel impersonation offering a complimentary stay. Calls to wireless numbers. Random auto-dialing. Wireless numbers never been in service or currently not in service.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 13 Jun 22 14:17 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #9274 0 seconds ago

Campaign: Hotel-ComplimentaryStay

Date/Time: 2022-06-09 17:21:42 +0000 UTC

To: +18136017272

From: +15616263969

Hotel impersonation offering a complimentary stay. Calls to wireless numbers. Random auto-dialing. Wireless numbers never been in service or currently not in service.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 13 Jun 22 14:23 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #9270 0 seconds ago

Campaign: Hotel-ComplimentaryStay

Date/Time: 2022-06-07 18:44:58 +0000 UTC

To: +12488975560

From: +17342940006

Hotel impersonation offering a complimentary stay. Calls to wireless numbers. Random auto-dialing. Wireless numbers never been in service or currently not in service.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 13 Jun 22 14:33 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #9269 0 seconds ago

Campaign: Hotel-ComplimentaryStay

Date/Time: 2022-06-07 00:03:06 +0000 UTC

To: +19139611066

From: +17852101752

Hotel impersonation offering a complimentary stay. Calls to wireless numbers. Random auto-dialing. Wireless numbers never been in service or currently not in service.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 13 Jun 22 14:53 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #9271 0 seconds ago

Campaign: Hotel-ComplimentaryStay

Date/Time: 2022-06-07 19:08:21 +0000 UTC

To: +16026478509

From: +16232435699

Hotel impersonation offering a complimentary stay. Calls to wireless numbers. Random auto-dialing. Wireless numbers never been in service or currently not in service.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 22 Jun 22 21:37 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #9427 0 seconds ago

Campaign: AutoWarranty-NationalDealerSvcs-P1

Date/Time: 2022-06-21 20:45:25 +0000 UTC

To: +18147066874

From: +16504902748

Automated, recorded voice calls to wireless numbers not permitted without consent. Numbers no longer in service or never been in service. Toll-free callback number not provided in voicemail.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 23 Jun 22 13:14 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #9430 0 seconds ago

Campaign:	Spanish-AutoWarranty-Upgrade
Date/Time:	2022-06-20 17:41:18 +0000 UTC
To:	+16517926396
From:	+15309824711

Pre-recorded calls with Spanish message regarding your vehicle service contract, last attempt to upgrade. Recorded voice calls to wireless numbers not permitted without consent. Numbers no longer in service or never been in service.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 24 Jun 22 13:52 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #9465 0 seconds ago

Campaign: SSA-P1-TexasFraud (GovtImpers)

Date/Time: 2022-06-23 23:05:23 +0000 UTC

To: +13524241478

From: +13524247948

FRAUD. Recorded message says SSN is suspended due to fraud in Texas or other state. Caller fraudulently claims to be from SSA. Spoofed caller-ID using random wireless and other USA subscriber numbers.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 29 Jun 22 15:12 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #9511 0 seconds ago

Campaign: LegalDept-Action-P1

Date/Time: 2022-06-23 18:11:05 +0000 UTC

To: +14056282527

From: +14056285995

Calls claiming to be from the Legal Department, advising about the recipient's case and how legal action will be taken against them. To speak to a federal agent they need to press one.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 29 Jun 22 17:45 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #9543 0 seconds ago

Campaign: Spanish-HealthInsCenter

Date/Time: 2022-06-22 22:24:38 +0000 UTC

To: +13867854535

From: +14075896477

Pre-recorded calls from the Health Insurance Center, to speak to agent press one. Automated calls to wireless numbers not permitted without consent. Numbers no longer in service or never been in service.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 29 Jun 22 18:49 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #9541 0 seconds ago

Campaign: Spanish-HealthInsCenter

Date/Time: 2022-06-21 22:24:04 +0000 UTC

To: +14322323954

From: +14327297905

Pre-recorded calls from the Health Insurance Center, to speak to agent press one. Automated calls to wireless numbers not permitted without consent. Numbers no longer in service or never been in service.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 30 Jun 22 16:12 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

[Redacted](#)

(URL is a private login; do not share.)

Call Details for Traceback #9551 0 seconds ago

Campaign: AutoWarranty-ExtendOrReinst
Date/Time: 2022-06-29 16:16:57 +0000 UTC
To: +18188075006
From: +18188062990

Recorded voice indicates offers to extend or reinstate vehicle warranty. Recorded message to mobile number. Some calls placed to numbers on national do-not-call list. Calls placed using many different Caller-ID values. Some identify the caller generically as Automotive Services; some voice-mail messages do not capture name of calling entity. Same calling numbers are regularly reported to FTC at donotcall.gov (over 100). We have previously been told caller has consent. Because this campaign routinely appears at the top of our daily tally of highest-volume robocallers, we periodically trace back examples to verify the source. Originator is asked to provide consent details for this call and to address failure to identify calling entity.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 30 Jun 22 16:21 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

[Redacted](#)

(URL is a private login; do not share.)

Call Details for Traceback #9553 0 seconds ago

Campaign: AutoWarranty-ExtendOrReinst
Date/Time: 2022-06-29 16:05:31 +0000 UTC
To: +18583545771
From: +18589252536

Recorded voice indicates offers to extend or reinstate vehicle warranty. Recorded message to mobile number. Some calls placed to numbers on national do-not-call list. Calls placed using many different Caller-ID values. Some identify the caller generically as Automotive Services; some voice-mail messages do not capture name of calling entity. Same calling numbers are regularly reported to FTC at donotcall.gov (over 100). We have previously been told caller has consent. Because this campaign routinely appears at the top of our daily tally of highest-volume robocallers, we periodically trace back examples to verify the source. Originator is asked to provide consent details for this call and to address failure to identify calling entity.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com

Date: 01 Jul 22 09:30 UTC

INDUSTRY TRACEBACK GROUP

Monthly Metrics - **Smartbiz Telecom, LLC**

NOC, you can find your organization's traceback-related metrics for the last 30 days below.

Your Summary:

Total Hops	Open	POE	Downstream	Orig	No Resp	Not Found	Avg Response	Campaigns
14	0	0	0	0	0	0	46 minutes 13 seconds	7

Upstream Summary:

Provider	Total Hops	Open	POE	Orig	No Resp	Not Found
Lata 1 Communications Inc.	2	1	1	0	0	0
Etelix.com USA, LLC	8	0	8	0	0	0
Telconus / Telcon US / Telcon Voice / Whisl	5	0	0	0	0	0

If you have any trouble seeing this email, please visit:

<https://portal.tracebacks.org/email-redirect?location=/providers/provider/summaries/386&userId=648&token=fb0ac696-fc95-49e8-8615-0c467c6e735f>

From: traceback-notice@tracebacks.org
To: katherine.rosales@smartbiztel.com
Date: 01 Jul 22 09:30 UTC

INDUSTRY TRACEBACK GROUP

Monthly Metrics - Smartbiz Telecom, LLC

noc, you can find your organization's traceback-related metrics for the last 30 days below.

Your Summary:

Total Hops	Open	POE	Downstream	Orig	No Resp	Not Found	Avg Response	Campaigns
14	0	0	0	0	0	0	46 minutes 13 seconds	7

Upstream Summary:

Provider	Total Hops	Open	POE	Orig	No Resp	Not Found
Lata 1 Communications Inc.	2	1	1	0	0	0
Etelix.com USA, LLC	8	0	8	0	0	0
Telconus / Telcon US / Telcon Voice / Whisl	5	0	0	0	0	0

If you have any trouble seeing this email, please visit:
<https://portal.tracebacks.org/email-redirect?location=/providers/provider/summaries/386&userId=10030&token=1d1334d7-c3bd-486a-8820-1b435937498f>

From: traceback-notice@tracebacks.org
To: eborrero@smartbiztel.com
Date: 01 Jul 22 09:30 UTC

INDUSTRY TRACEBACK GROUP

Monthly Metrics - **Smartbiz Telecom, LLC**

Eduardo Borrero, you can find your organization's traceback-related metrics for the last 30 days below.

Your Summary:

Total Hops	Open	POE	Downstream	Orig	No Resp	Not Found	Avg Response	Campaigns
14	0	0	0	0	0	0	46 minutes 13 seconds	7

Upstream Summary:

Provider	Total Hops	Open	POE	Orig	No Resp	Not Found
Lata 1 Communications Inc.	2	1	1	0	0	0
Etelix.com USA, LLC	8	0	8	0	0	0
Telconus / Telcon US / Telcon Voice / Whisl	5	0	0	0	0	0

If you have any trouble seeing this email, please visit:
<https://portal.tracebacks.org/email-redirect?location=/providers/provider/summaries/386&userId=11201&token=4edf3f65-0c91-4235-b656-630c346c1097>

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 01 Jul 22 14:56 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #9588 0 seconds ago

Campaign: Discount-DirecTV50

Date/Time: 2022-06-30 18:25:05 +0000 UTC

To: +12533321444

From: +13614629177

FRAUD. Caller claims to be from ATT DirecTV offering 50 percent discount and may request callback. Calls are NOT from DirectTV; caller will attempt to extort money via prepayment. Recorded message to mobile number not allowed.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 01 Jul 22 15:03 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #9579 0 seconds ago

Campaign: Discount-DirecTV50

Date/Time: 2022-06-30 18:29:55 +0000 UTC

To: +14402137689

From: +16184774662

FRAUD. Caller claims to be from ATT DirecTV offering 50 percent discount and may request callback. Calls are NOT from DirectTV; caller will attempt to extort money via prepayment. Recorded message to mobile number not allowed.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 14 Jul 22 06:18 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #9708 0 seconds ago

Campaign: GovtImpers

Date/Time: 2022-07-08 14:38:00 +0000 UTC

To: +18568319478

From: +18775277867

Calls impersonating law enforcement or government officials. Making false statements to possibly extract payment or personal information.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 15 Jul 22 14:44 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #9727 0 seconds ago

Campaign: Hotel-ComplimentaryStay

Date/Time: 2022-07-12 23:24:03 +0000 UTC

To: +19518099928

From: +15626956435

Hotel impersonation offering a complimentary stay. Calls to wireless numbers. Random auto-dialing. Wireless numbers never been in service or currently not in service.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 15 Jul 22 14:59 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #9721 0 seconds ago

Campaign: LegalDept-Action-P1

Date/Time: 2022-07-14 17:05:04 +0000 UTC

To: +13362540939

From: +13366903666

Calls claiming to be from the Legal Department, advising about the recipient's case and how legal action will be taken against them. To speak to a federal agent they need to press one.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 15 Jul 22 14:59 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

[Redacted](#)

(URL is a private login; do not share.)

Call Details for Traceback #9722 0 seconds ago

Campaign: LegalDept-Action-P1

Date/Time: 2022-07-14 16:41:43 +0000 UTC

To: +19032446829

From: +19036126146

Calls claiming to be from the Legal Department, advising about the recipient's case and how legal action will be taken against them. To speak to a federal agent they need to press one.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 15 Jul 22 15:00 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #9726 0 seconds ago

Campaign: Hotel-ComplimentaryStay

Date/Time: 2022-07-12 01:13:15 +0000 UTC

To: +14234026248

From: +16153606853

Hotel impersonation offering a complimentary stay. Calls to wireless numbers. Random auto-dialing. Wireless numbers never been in service or currently not in service.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 15 Jul 22 15:12 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #9728 0 seconds ago

Campaign: Hotel-ComplimentaryStay

Date/Time: 2022-07-13 00:39:46 +0000 UTC

To: +16604923927

From: +13142822499

Hotel impersonation offering a complimentary stay. Calls to wireless numbers. Random auto-dialing. Wireless numbers never been in service or currently not in service.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 15 Jul 22 15:33 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

[Redacted](#)

(URL is a private login; do not share.)

Call Details for Traceback #9720 0 seconds ago

Campaign: LegalDept-Action-P1

Date/Time: 2022-07-14 18:16:39 +0000 UTC

To: +14693659631

From: +14697379452

Calls claiming to be from the Legal Department, advising about the recipient's case and how legal action will be taken against them. To speak to a federal agent they need to press one.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 15 Jul 22 15:34 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

[Redacted](#)

(URL is a private login; do not share.)

Call Details for Traceback #9719 0 seconds ago

Campaign: LegalDept-Action-P1

Date/Time: 2022-07-14 18:19:20 +0000 UTC

To: +15019440512

From: +15019087422

Calls claiming to be from the Legal Department, advising about the recipient's case and how legal action will be taken against them. To speak to a federal agent they need to press one.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 15 Jul 22 16:45 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #9724 0 seconds ago

Campaign: Hotel-ComplimentaryStay

Date/Time: 2022-07-11 21:00:07 +0000 UTC

To: +15745272339

From: +12605571382

Hotel impersonation offering a complimentary stay. Calls to wireless numbers. Random auto-dialing. Wireless numbers never been in service or currently not in service.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 18 Jul 22 12:03 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #9725 0 seconds ago

Campaign: Hotel-ComplimentaryStay

Date/Time: 2022-07-11 19:47:37 +0000 UTC

To: +14354145837

From: +18019229383

Hotel impersonation offering a complimentary stay. Calls to wireless numbers. Random auto-dialing. Wireless numbers never been in service or currently not in service.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 22 Jul 22 14:25 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #9822 0 seconds ago

Campaign: CCIRR-Expire
Date/Time: 2022-07-21 20:10:11 +0000 UTC
To: +17606083091
From: +17609913564

Spoofed calls claiming to be financial institution advising your eligibility for rate reduction is about to expire.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 22 Jul 22 22:11 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #9820 0 seconds ago

Campaign: CCIRR-Expire
Date/Time: 2022-07-20 22:52:51 +0000 UTC
To: +16177924618
From: +18012806451

Spoofed calls claiming to be financial institution advising your eligibility for rate reduction is about to expire.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 22 Jul 22 22:12 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #9823 0 seconds ago

Campaign: CCIRR-Expire

Date/Time: 2022-07-21 16:29:10 +0000 UTC

To: +18132947767

From: +18635713684

Spoofed calls claiming to be financial institution advising your eligibility for rate reduction is about to expire.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 27 Jul 22 21:42 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #9877 0 seconds ago

Campaign: Financial-Hardship-P3

Date/Time: 2022-07-26 16:11:00 +0000 UTC

To: +16189363175

From: +17156490874

Pre-recorded call offering assistance program to eliminate financial hardship. Evidence suggesting lack of consent, including consumer complaints, honeypot data, and other information.

From: traceback-notice@tracebacks.org
To: eborrero@smartbiztel.com
Date: 01 Aug 22 09:31 UTC

INDUSTRY TRACEBACK GROUP

Monthly Metrics - **Smartbiz Telecom, LLC**

Eduardo Borrero, you can find your organization's traceback-related metrics for the last 30 days below.

Your Summary:

Total Hops	Open	POE	Downstream	Orig	No Resp	Not Found	Avg Response	Campaigns
13	0	0	0	0	0	2	10 hours 16 minutes	4

Upstream Summary:

Provider	Total Hops	Open	POE	Orig	No Resp	Not Found
Lata 1 Communications Inc.	5	0	5	0	0	0
Red Telecom LLC	1	0	0	0	0	0
Telconus / Telcon US / Telcon Voice / Whisl	6	0	0	0	0	0

If you have any trouble seeing this email, please visit:

<https://portal.tracebacks.org/email-redirect?location=/providers/provider/summaries/386&userId=11201&token=0a521a33-ef26-4871-9a06-b4792c36c58c>

From: traceback-notice@tracebacks.org
To: noc@smartbiztel.com
Date: 01 Aug 22 09:31 UTC

INDUSTRY TRACEBACK GROUP

Monthly Metrics - **Smartbiz Telecom, LLC**

NOC, you can find your organization's traceback-related metrics for the last 30 days below.

Your Summary:

Total Hops	Open	POE	Downstream	Orig	No Resp	Not Found	Avg Response	Campaigns
13	0	0	0	0	0	2	10 hours 16 minutes	4

Upstream Summary:

Provider	Total Hops	Open	POE	Orig	No Resp	Not Found
Lata 1 Communications Inc.	5	0	5	0	0	0
Red Telecom LLC	1	0	0	0	0	0
Telconus / Telcon US / Telcon Voice / Whisl	6	0	0	0	0	0

If you have any trouble seeing this email, please visit:
<https://portal.tracebacks.org/email-redirect?location=/providers/provider/summaries/386&userId=648&token=708a54ab-bbd2-4849-9a2f-1e1efb2dfb42>

From: traceback-notice@tracebacks.org
To: katherine.rosales@smartbiztel.com
Date: 01 Aug 22 09:31 UTC

INDUSTRY TRACEBACK GROUP

Monthly Metrics - **Smartbiz Telecom, LLC**

noc, you can find your organization's traceback-related metrics for the last 30 days below.

Your Summary:

Total Hops	Open	POE	Downstream	Orig	No Resp	Not Found	Avg Response	Campaigns
13	0	0	0	0	0	2	10 hours 16 minutes	4

Upstream Summary:

Provider	Total Hops	Open	POE	Orig	No Resp	Not Found
Lata 1 Communications Inc.	5	0	5	0	0	0
Red Telecom LLC	1	0	0	0	0	0
Telconus / Telcon US / Telcon Voice / Whisl	6	0	0	0	0	0

If you have any trouble seeing this email, please visit:

<https://portal.tracebacks.org/email-redirect?location=/providers/provider/summaries/386&userId=10030&token=b71f72da-27d2-4cde-9b9b-b4332103c531>

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 02 Aug 22 17:27 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #9934 0 seconds ago

Campaign: Discount-DirecTV50

Date/Time: 2022-08-01 19:25:21 +0000 UTC

To: +14792632690

From: +19014130935

FRAUD. Caller claims to be from ATT DirecTV offering 50 percent discount and may request callback. Calls are NOT from DirectTV; caller will attempt to extort money via prepayment. Recorded message to mobile number not allowed.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 05 Aug 22 15:02 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #9994 0 seconds ago

Campaign: DebtRelief-ZeroTax

Date/Time: 2022-08-03 21:34:08 +0000 UTC

To: +16058585125

From: +17158005069

Pre-recorded call regarding new zero tax debt relief program. Automated calls to wireless numbers generally not permitted. Calls to numbers not in service.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 05 Aug 22 15:09 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #9995 0 seconds ago

Campaign: DebtRelief-ZeroTax

Date/Time: 2022-08-03 21:08:11 +0000 UTC

To: +14234134359

From: +14632446043

Pre-recorded call regarding new zero tax debt relief program. Automated calls to wireless numbers generally not permitted. Calls to numbers not in service.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 05 Aug 22 15:18 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #9993 0 seconds ago

Campaign: DebtRelief-ZeroTax

Date/Time: 2022-08-03 21:58:06 +0000 UTC

To: +12058600784

From: +15632878638

Pre-recorded call regarding new zero tax debt relief program. Automated calls to wireless numbers generally not permitted. Calls to numbers not in service.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 05 Aug 22 15:48 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #9991 0 seconds ago

Campaign: DebtRelief-ZeroTax

Date/Time: 2022-08-03 22:40:14 +0000 UTC

To: +18649347599

From: +12173501814

Pre-recorded call regarding new zero tax debt relief program. Automated calls to wireless numbers generally not permitted. Calls to numbers not in service.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 05 Aug 22 15:50 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #9990 0 seconds ago

Campaign: DebtRelief-ZeroTax

Date/Time: 2022-08-03 22:56:48 +0000 UTC

To: +14236934775

From: +12098447654

Pre-recorded call regarding new zero tax debt relief program. Automated calls to wireless numbers generally not permitted. Calls to numbers not in service.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 08 Aug 22 18:42 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

[Redacted](#)

(URL is a private login; do not share.)

Call Details for Traceback #9992 0 seconds ago

Campaign: DebtRelief-ZeroTax

Date/Time: 2022-08-03 22:27:14 +0000 UTC

To: +14234134359

From: +19209811319

Pre-recorded call regarding new zero tax debt relief program. Automated calls to wireless numbers generally not permitted. Calls to numbers not in service.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 11 Aug 22 16:48 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #10058 0 seconds ago

Campaign: AutoWarranty-Various-P3

Date/Time: 2022-08-08 15:14:00 +0000 UTC

To: +15099445289

From: +13606566593

Caller offering some type of car warranty. Typically using a prerecorded or artificial voice. Some calls are to mobiles. May not honor DNC.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 15 Aug 22 13:41 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #10087 0 seconds ago

Campaign: Tax-Debt-P1

Date/Time: 2022-08-10 15:32:57 +0000 UTC

To: +15059167890

From: +17372640665

Prerecorded calls claiming recipient inquired for assistance on their IRS tax debt. Caller doesn't identify who they are. Automated calls to wireless numbers not permitted without consent. Numbers no longer in service or never been in service.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 15 Aug 22 13:43 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

[Redacted](#)

(URL is a private login; do not share.)

Call Details for Traceback #10088 0 seconds ago

Campaign: Tax-Debt-P1

Date/Time: 2022-08-10 22:45:08 +0000 UTC

To: +18609415444

From: +12345624415

Prerecorded calls claiming recipient inquired for assistance on their IRS tax debt. Caller doesn't identify who they are. Automated calls to wireless numbers not permitted without consent. Numbers no longer in service or never been in service.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 15 Aug 22 15:38 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

[Redacted](#)

(URL is a private login; do not share.)

Call Details for Traceback #10089 0 seconds ago

Campaign: Tax-Debt-P1

Date/Time: 2022-08-11 22:23:15 +0000 UTC

To: +14797215403

From: +18317132087

Prerecorded calls claiming recipient inquired for assistance on their IRS tax debt. Caller doesn't identify who they are. Automated calls to wireless numbers not permitted without consent. Numbers no longer in service or never been in service.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 15 Aug 22 16:43 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #10086 0 seconds ago

Campaign: Tax-Debt-P1

Date/Time: 2022-08-11 19:04:15 +0000 UTC

To: +15415914470

From: +13463727634

Prerecorded calls claiming recipient inquired for assistance on their IRS tax debt. Caller doesn't identify who they are. Automated calls to wireless numbers not permitted without consent. Numbers no longer in service or never been in service.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 15 Aug 22 19:07 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #10085 0 seconds ago

Campaign: Tax-Debt-P1

Date/Time: 2022-08-11 18:40:36 +0000 UTC

To: +15418529035

From: +19519012074

Prerecorded calls claiming recipient inquired for assistance on their IRS tax debt. Caller doesn't identify who they are. Automated calls to wireless numbers not permitted without consent. Numbers no longer in service or never been in service.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 19 Aug 22 14:13 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #10162 0 seconds ago

Campaign: Tax-Debt-P1

Date/Time: 2022-08-15 19:35:40 +0000 UTC

To: +16627030343

From: +17177084591

Prerecorded calls claiming recipient inquired for assistance on their IRS tax debt. Caller doesn't identify who they are. Automated calls to wireless numbers not permitted without consent. Numbers no longer in service or never been in service.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 19 Aug 22 15:07 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

[Redacted](#)

(URL is a private login; do not share.)

Call Details for Traceback #10163 0 seconds ago

Campaign: Tax-Debt-P1

Date/Time: 2022-08-17 15:31:56 +0000 UTC

To: +16626643872

From: +13866660541

Prerecorded calls claiming recipient inquired for assistance on their IRS tax debt. Caller doesn't identify who they are. Automated calls to wireless numbers not permitted without consent. Numbers no longer in service or never been in service.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 19 Aug 22 15:09 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #10165 0 seconds ago

Campaign: Tax-Debt-P1

Date/Time: 2022-08-17 22:04:35 +0000 UTC

To: +14844085907

From: +17072044228

Prerecorded calls claiming recipient inquired for assistance on their IRS tax debt. Caller doesn't identify who they are. Automated calls to wireless numbers not permitted without consent. Numbers no longer in service or never been in service.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 19 Aug 22 15:11 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #10159 0 seconds ago

Campaign: Tax-Debt-P1

Date/Time: 2022-08-16 19:51:58 +0000 UTC

To: +14752433534

From: +17793231211

Prerecorded calls claiming recipient inquired for assistance on their IRS tax debt. Caller doesn't identify who they are. Automated calls to wireless numbers not permitted without consent. Numbers no longer in service or never been in service.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 19 Aug 22 17:46 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #10167 0 seconds ago

Campaign: Tax-Debt-P1

Date/Time: 2022-08-17 16:02:31 +0000 UTC

To: +13136709416

From: +15206500763

Prerecorded calls claiming recipient inquired for assistance on their IRS tax debt. Caller doesn't identify who they are. Automated calls to wireless numbers not permitted without consent. Numbers no longer in service or never been in service.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 19 Aug 22 17:50 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

[Redacted](#)

(URL is a private login; do not share.)

Call Details for Traceback #10160 0 seconds ago

Campaign: Tax-Debt-P1

Date/Time: 2022-08-16 17:16:05 +0000 UTC

To: +18283370569

From: +18509550193

Prerecorded calls claiming recipient inquired for assistance on their IRS tax debt. Caller doesn't identify who they are. Automated calls to wireless numbers not permitted without consent. Numbers no longer in service or never been in service.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 19 Aug 22 17:56 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #10161 0 seconds ago

Campaign: Tax-Debt-P1

Date/Time: 2022-08-16 21:10:48 +0000 UTC

To: +12529083863

From: +16099938744

Prerecorded calls claiming recipient inquired for assistance on their IRS tax debt. Caller doesn't identify who they are. Automated calls to wireless numbers not permitted without consent. Numbers no longer in service or never been in service.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 20 Aug 22 12:26 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

[Redacted](#)

(URL is a private login; do not share.)

Call Details for Traceback #10166 0 seconds ago

Campaign: Tax-Debt-P1
Date/Time: 2022-08-17 15:43:05 +0000 UTC
To: +12315193509
From: +13855660650

Prerecorded calls claiming recipient inquired for assistance on their IRS tax debt. Caller doesn't identify who they are. Automated calls to wireless numbers not permitted without consent. Numbers no longer in service or never been in service.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 20 Aug 22 12:28 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #10164 0 seconds ago

Campaign: Tax-Debt-P1

Date/Time: 2022-08-17 20:57:44 +0000 UTC

To: +18147794654

From: +12097642412

Prerecorded calls claiming recipient inquired for assistance on their IRS tax debt. Caller doesn't identify who they are. Automated calls to wireless numbers not permitted without consent. Numbers no longer in service or never been in service.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 24 Aug 22 16:19 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

[Redacted](#)

(URL is a private login; do not share.)

Call Details for Traceback #10224 0 seconds ago

Campaign: StudentLoan-Payments
Date/Time: 2022-08-23 18:56:00 +0000 UTC
To: +14437133457
From: +15302170777

Calls to recipients about student loan payment suspension. Voice-mail message does not identify the calling entity, nor does it provide an opt-out option. Evidence suggesting lack of consent, including consumer complaints, honeypot data, and other information.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 25 Aug 22 14:06 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #10237 0 seconds ago

Campaign: StudentLoan-Payments-P1
Date/Time: 2022-08-24 19:02:24 +0000 UTC
To: +18607984114
From: +15415815549

Calls to recipients about student loan payment suspension. Voice-mail message does not identify the calling entity. Evidence suggesting lack of consent, including consumer complaints, honeypot data, and other information.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 25 Aug 22 16:13 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #10231 0 seconds ago

Campaign: StudentLoan-Payments-P1
Date/Time: 2022-08-24 17:38:36 +0000 UTC
To: +15054002808
From: +19728450350

Calls to recipients about student loan payment suspension. Voice-mail message does not identify the calling entity. Evidence suggesting lack of consent, including consumer complaints, honeypot data, and other information.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 25 Aug 22 16:18 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

[Redacted](#)

(URL is a private login; do not share.)

Call Details for Traceback #10236 0 seconds ago

Campaign: StudentLoan-Payments-P1
Date/Time: 2022-08-24 16:30:02 +0000 UTC
To: +16038920087
From: +16412892883

Calls to recipients about student loan payment suspension. Voice-mail message does not identify the calling entity. Evidence suggesting lack of consent, including consumer complaints, honeypot data, and other information.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 26 Aug 22 19:18 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #10239 0 seconds ago

Campaign: StudentLoan-Payments-P1
Date/Time: 2022-08-24 15:34:47 +0000 UTC
To: +16014702824
From: +16264065470

Calls to recipients about student loan payment suspension. Voice-mail message does not identify the calling entity. Evidence suggesting lack of consent, including consumer complaints, honeypot data, and other information.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 30 Aug 22 15:12 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #10293 0 seconds ago

Campaign: StudentLoan-Payments-P1
Date/Time: 2022-08-29 19:26:07 +0000 UTC
To: +13174522049
From: +14352964843

Calls to recipients about student loan payment suspension. Voice-mail message does not identify the calling entity. Evidence suggesting lack of consent, including consumer complaints, honeypot data, and other information.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 30 Aug 22 15:14 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #10292 0 seconds ago

Campaign: StudentLoan-Payments-P1
Date/Time: 2022-08-29 19:31:51 +0000 UTC
To: +13107351566
From: +19143871062

Calls to recipients about student loan payment suspension. Voice-mail message does not identify the calling entity. Evidence suggesting lack of consent, including consumer complaints, honeypot data, and other information.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 30 Aug 22 15:17 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #10294 0 seconds ago

Campaign: StudentLoan-Payments-P1
Date/Time: 2022-08-29 18:41:44 +0000 UTC
To: +18504961809
From: +16828990913

Calls to recipients about student loan payment suspension. Voice-mail message does not identify the calling entity. Evidence suggesting lack of consent, including consumer complaints, honeypot data, and other information.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 30 Aug 22 16:20 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #10297 0 seconds ago

Campaign: StudentLoan-Payments-P1
Date/Time: 2022-08-29 17:44:30 +0000 UTC
To: +18315780357
From: +16612491810

Calls to recipients about student loan payment suspension. Voice-mail message does not identify the calling entity. Evidence suggesting lack of consent, including consumer complaints, honeypot data, and other information.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 30 Aug 22 20:31 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #10298 0 seconds ago

Campaign: StudentLoan-Payments-P1
Date/Time: 2022-08-29 15:23:46 +0000 UTC
To: +13479613682
From: +17075171309

Calls to recipients about student loan payment suspension. Voice-mail message does not identify the calling entity. Evidence suggesting lack of consent, including consumer complaints, honeypot data, and other information.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 31 Aug 22 14:03 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #10299 0 seconds ago

Campaign: StudentLoan-Payments-P1
Date/Time: 2022-08-29 15:15:40 +0000 UTC
To: +13479423130
From: +15303317802

Calls to recipients about student loan payment suspension. Voice-mail message does not identify the calling entity. Evidence suggesting lack of consent, including consumer complaints, honeypot data, and other information.

From: traceback-notice@tracebacks.org
To: noc@smartbiztel.com
Date: 01 Sep 22 09:30 UTC

INDUSTRY TRACEBACK GROUP

Monthly Metrics - Smartbiz Telecom, LLC

NOC, you can find your organization's traceback-related metrics for the last 30 days below.

Your Summary:

Total Hops	Open	POE	Downstream	Orig	No Resp	Not Found	Avg Response	Campaigns
32	0	0	0	0	0	1	1 hour 4 minutes	5

Upstream Summary:

Provider	Total Hops	Open	POE	Orig	No Resp	Not Found
Telconus / Telcon US / Telcon Voice / Whisl	32	0	0	0	0	0

If you have any trouble seeing this email, please visit:
<https://portal.tracebacks.org/email-redirect?location=/providers/provider/summaries/386&userId=648&token=b6a0ed80-b980-492c-83f3-864a1fe8cfbd>

From: traceback-notice@tracebacks.org
To: eborrero@smartbiztel.com
Date: 01 Sep 22 09:30 UTC

INDUSTRY TRACEBACK GROUP

Monthly Metrics - Smartbiz Telecom, LLC

Eduardo Borrero, you can find your organization's traceback-related metrics for the last 30 days below.

Your Summary:

Total Hops	Open	POE	Downstream	Orig	No Resp	Not Found	Avg Response	Campaigns
32	0	0	0	0	0	1	1 hour 4 minutes	5

Upstream Summary:

Provider	Total Hops	Open	POE	Orig	No Resp	Not Found
Telconus / Telcon US / Telcon Voice / Whisl	32	0	0	0	0	0

If you have any trouble seeing this email, please visit:
<https://portal.tracebacks.org/email-redirect?location=/providers/provider/summaries/386&userId=11201&token=6341df64-ab79-4674-b01d-f52d722259f3>

From: traceback-notice@tracebacks.org
To: katherine.rosales@smartbiztel.com
Date: 01 Sep 22 09:30 UTC

INDUSTRY TRACEBACK GROUP

Monthly Metrics - Smartbiz Telecom, LLC

noc, you can find your organization's traceback-related metrics for the last 30 days below.

Your Summary:

Total Hops	Open	POE	Downstream	Orig	No Resp	Not Found	Avg Response	Campaigns
32	0	0	0	0	0	1	1 hour 4 minutes	5

Upstream Summary:

Provider	Total Hops	Open	POE	Orig	No Resp	Not Found
Telconus / Telcon US / Telcon Voice / Whisl	32	0	0	0	0	0

If you have any trouble seeing this email, please visit:
<https://portal.tracebacks.org/email-redirect?location=/providers/provider/summaries/386&userId=10030&token=bca8ad43-7493-4837-925d-985162da124c>

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 01 Sep 22 16:32 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #10352 0 seconds ago

Campaign: StudentLoan-ForgivenessCenter

Date/Time: 2022-08-31 18:09:53 +0000 UTC

To: +12037459184

From: +17328271944

Call to mobile using pre-recorded voice. Referencing student loan Forgiveness center; Some call recipients do not have student loans.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 01 Sep 22 16:38 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

[Redacted](#)

(URL is a private login; do not share.)

Call Details for Traceback #10349 0 seconds ago

Campaign: StudentLoan-ForgivenessCenter

Date/Time: 2022-08-26 17:22:27 +0000 UTC

To: +16039309928

From: +17753075151

Call to mobile using pre-recorded voice. Referencing student loan Forgiveness center; Some call recipients do not have student loans.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 01 Sep 22 16:44 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #10357 0 seconds ago

Campaign: StudentLoan-ForgivenessCenter

Date/Time: 2022-08-29 16:39:04 +0000 UTC

To: +17342181848

From: +17324120791

Call to mobile using pre-recorded voice. Referencing student loan Forgiveness center; Some call recipients do not have student loans.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 01 Sep 22 16:50 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #10358 0 seconds ago

Campaign: StudentLoan-ForgivenessCenter

Date/Time: 2022-08-30 16:28:13 +0000 UTC

To: +12486335519

From: +16056004814

Call to mobile using pre-recorded voice. Referencing student loan Forgiveness center; Some call recipients do not have student loans.

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 14 Sep 22 17:24 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

Redacted

(URL is a private login; do not share.)

Call Details for Traceback #10480 0 seconds ago

Campaign: Amazon-AuthorizeOrder

Date/Time: 2022-09-12 17:45:09 +0000 UTC

To: +15867093862

From: +15864056881

Calls to wireless numbers impersonating Amazon, calling to authorize an order that was placed.

*This email was sent from a notification-only address that does not accept incoming email. Please do not reply to this message - send inquiries to **support@traceback.org***

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 21 Sep 22 15:18 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:
<https://portal.tracebacks.org/hops/hop/57360>
(URL is a private login; do not share.)

Call Details for Traceback #10579 0 seconds ago

Campaign: CaresAct-PandemicRefund

Date/Time: 2022-09-14 18:50:00 +0000 UTC

To: +12124168455

From: +15418375559

Calls to recipient advising their business is eligible under the CARES Act to receive compensation for employees retained during the pandemic. Recipient doesn't own a business.

This email was sent from a notification-only address that does not accept incoming email. Please do not reply to this message - send inquiries to support@tracebacks.org

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 21 Sep 22 18:55 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:
<https://portal.tracebacks.org/hops/hop/57386>
(URL is a private login; do not share.)

Call Details for Traceback #10580 0 seconds ago

Campaign: CaresAct-PandemicRefund

Date/Time: 2022-09-21 15:00:00 +0000 UTC

To: +12124168455

From: +13465156123

Calls to recipient advising their business is eligible under the CARES Act to receive compensation for employees retained during the pandemic. Recipient doesn't own a business.

This email was sent from a notification-only address that does not accept incoming email. Please do not reply to this message - send inquiries to support@tracebacks.org

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 22 Sep 22 14:15 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:
<https://portal.tracebacks.org/hops/hop/57437>
(URL is a private login; do not share.)

Call Details for Traceback #10592 0 seconds ago

Campaign: AutoWarranty-Variious-P2

Date/Time: 2022-09-19 15:19:19 +0000 UTC

To: +17329911318

From: +17322097942

Caller offering some type of car warranty. Using a prerecorded or artificial voice. Calls to wireless numbers. Random auto-dialing. Wireless numbers never been in service or currently not in service.

This email was sent from a notification-only address that does not accept incoming email. Please do not reply to this message - send inquiries to support@tracebacks.org

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 30 Sep 22 19:41 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:
<https://portal.tracebacks.org/hops/hop/58061>
(URL is a private login; do not share.)

Call Details for Traceback #10711 0 seconds ago

Campaign: AutoWarranty-Variious-P2

Date/Time: 2022-09-26 15:15:37 +0000 UTC

To: +12316909525

From: +12312618921

Caller offering some type of car warranty. Using a prerecorded or artificial voice. Calls to wireless numbers. Random auto-dialing. Wireless numbers never been in service or currently not in service.

This email was sent from a notification-only address that does not accept incoming email. Please do not reply to this message - send inquiries to support@tracebacks.org

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 01 Oct 22 09:30 UTC

INDUSTRY TRACEBACK GROUP

Monthly Metrics - **Smartbiz Telecom, LLC**

[Redacted], you can find your organization's traceback-related metrics for the last 30 days below.

Your Summary:

Total Hops	Open	POE	Downstream	Orig	No Resp	Not Found	Avg Response	Campaigns
7	0	0	0	0	0	0	56 minutes 23 seconds	3

Upstream Summary:

This table shows the providers who you have identified as an upstream provider in response to tracebacks. The chart displays the number of occurrences in which each of those providers is the Point of Entry, Origin, non-responsive, or was unable to find the call. The information presented only includes the tracebacks where you identified the listed providers; the providers may also have appeared in these positions for other tracebacks as well.

Provider	Total Hops	Open	POE	Orig	No Resp	Not Found
Red Telecom LLC	2	0	0	0	0	0
Telconus / Telcon US / Telcon Voice / Whisl	7	0	0	0	0	0

If you have any trouble seeing this email, please visit:
<https://portal.tracebacks.org/providers/provider/summaries/386>

*This email was sent from a notification-only address that does not accept incoming email. Please do not reply to this message - send inquiries to **support@tracebacks.org***

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 04 Oct 22 15:41 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:
<https://portal.tracebacks.org/hops/hop/58185>
(URL is a private login; do not share.)

Call Details for Traceback #10737 0 seconds ago

Campaign: Amazon-AuthorizeOrder

Date/Time: 2022-10-03 19:39:02 +0000 UTC

To: +15868714404

From: +16075352916

Calls to wireless numbers impersonating Amazon, calling to authorize an order that was placed.

*This email was sent from a notification-only address that does not accept incoming email. Please do not reply to this message - send inquiries to **support@tracebacks.org***

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 07 Oct 22 15:36 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:
<https://portal.tracebacks.org/hops/hop/58406>
(URL is a private login; do not share.)

Call Details for Traceback #10767 0 seconds ago

Campaign: Discount-Avail50%

Date/Time: 2022-10-06 15:30:43 +0000 UTC

To: +18025355702

From: +17188775059

Calls claiming to be an Internet/TV provider offering 50% discount to recipient. Automated calls to wireless numbers generally not permitted.

This email was sent from a notification-only address that does not accept incoming email. Please do not reply to this message - send inquiries to support@tracebacks.org

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 12 Oct 22 17:18 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:
<https://portal.tracebacks.org/hops/hop/58681>
(URL is a private login; do not share.)

Call Details for Traceback #10810 0 seconds ago

Campaign: StudentLoan-Payments-P1

Date/Time: 2022-10-11 15:42:35 +0000 UTC

To: +19292588900

From: +12205003129

Calls to recipients about student loan payment dismissal and/or suspension. Voice-mail message does not identify the calling entity. Evidence suggesting lack of consent, including consumer complaints, honeypot data, and other information.

This email was sent from a notification-only address that does not accept incoming email. Please do not reply to this message - send inquiries to support@tracebacks.org

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 12 Oct 22 17:20 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:
<https://portal.tracebacks.org/hops/hop/58683>
(URL is a private login; do not share.)

Call Details for Traceback #10811 0 seconds ago

Campaign: StudentLoan-Payments-P1

Date/Time: 2022-10-11 16:25:09 +0000 UTC

To: +19173402555

From: +15303882927

Calls to recipients about student loan payment dismissal and/or suspension. Voice-mail message does not identify the calling entity. Evidence suggesting lack of consent, including consumer complaints, honeypot data, and other information.

This email was sent from a notification-only address that does not accept incoming email. Please do not reply to this message - send inquiries to support@tracebacks.org

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 12 Oct 22 18:16 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:
<https://portal.tracebacks.org/hops/hop/58702>
(URL is a private login; do not share.)

Call Details for Traceback #10809 0 seconds ago

Campaign: StudentLoan-Payments-P1

Date/Time: 2022-10-11 22:31:55 +0000 UTC

To: +15869447935

From: +15307371340

Calls to recipients about student loan payment dismissal and/or suspension. Voice-mail message does not identify the calling entity. Evidence suggesting lack of consent, including consumer complaints, honeypot data, and other information.

This email was sent from a notification-only address that does not accept incoming email. Please do not reply to this message - send inquiries to support@tracebacks.org

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 17 Oct 22 15:50 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:
<https://portal.tracebacks.org/hops/hop/58936>
(URL is a private login; do not share.)

Call Details for Traceback #10862 0 seconds ago

Campaign: Discount-Avail50%

Date/Time: 2022-10-15 19:38:43 +0000 UTC

To: +14795025872

From: +13053569999

Calls claiming to be an Internet/TV provider offering 50% discount to recipient. Automated calls to wireless numbers generally not permitted.

This email was sent from a notification-only address that does not accept incoming email. Please do not reply to this message - send inquiries to support@tracebacks.org

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 28 Oct 22 18:40 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:
<https://portal.tracebacks.org/hops/hop/59889>
(URL is a private login; do not share.)

Call Details for Traceback #11028 0 seconds ago

Campaign: StudentLoan-\$10,000-Removal
Date/Time: 2022-10-27 22:00:27 +0000 UTC
To: +19083241637
From: +19457770768

Calls to recipients advising their student loan is now eligible for a \$10,000 removal on their account. Recipients may not have student loans. Evidence suggesting lack of consent, including consumer complaints and other information.

This email was sent from a notification-only address that does not accept incoming email. Please do not reply to this message - send inquiries to support@tracebacks.org

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 31 Oct 22 14:56 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:
<https://portal.tracebacks.org/hops/hop/59974>
(URL is a private login; do not share.)

Call Details for Traceback #11038 0 seconds ago

Campaign: StudentLoan-\$10,000-Removal
Date/Time: 2022-10-28 14:13:27 +0000 UTC
To: +18706270066
From: +16282009162

Calls to recipients advising their student loan is now eligible for a \$10,000/\$20,000 removal on their account. Recipients may not have student loans. Evidence suggesting lack of consent, including consumer complaints and other information.

This email was sent from a notification-only address that does not accept incoming email. Please do not reply to this message - send inquiries to support@tracebacks.org

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 31 Oct 22 14:58 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:
<https://portal.tracebacks.org/hops/hop/59975>
(URL is a private login; do not share.)

Call Details for Traceback #11040 0 seconds ago

Campaign: StudentLoan-\$10,000-Removal
Date/Time: 2022-10-28 15:40:41 +0000 UTC
To: +15014258332
From: +18454728677

Calls to recipients advising their student loan is now eligible for a \$10,000/\$20,000 removal on their account. Recipients may not have student loans. Evidence suggesting lack of consent, including consumer complaints and other information.

This email was sent from a notification-only address that does not accept incoming email. Please do not reply to this message - send inquiries to support@tracebacks.org

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 31 Oct 22 16:24 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:
<https://portal.tracebacks.org/hops/hop/60006>
(URL is a private login; do not share.)

Call Details for Traceback #11042 0 seconds ago

Campaign: StudentLoan-\$10,000-Removal
Date/Time: 2022-10-28 15:47:45 +0000 UTC
To: +12293447986
From: +19143357026

Calls to recipients advising their student loan is now eligible for a \$10,000/\$20,000 removal on their account. Recipients may not have student loans. Evidence suggesting lack of consent, including consumer complaints and other information.

This email was sent from a notification-only address that does not accept incoming email. Please do not reply to this message - send inquiries to support@tracebacks.org

From: traceback-notice@tracebacks.org
To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com
Date: 01 Nov 22 09:30 UTC

INDUSTRY TRACEBACK GROUP

Monthly Metrics - **Smartbiz Telecom, LLC**

[Redacted], you can find your organization's traceback-related metrics for the last 30 days below.

Your Summary:

Total Hops	Open	POE	Downstream	Orig	No Resp	Not Found	Avg Response	Campaigns
10	1	0	0	0	0	0	2 hours 34 minutes	4

Upstream Summary:

This table shows the providers who you have identified as an upstream provider in response to tracebacks. The chart displays the number of occurrences in which each of those providers is the Point of Entry, Origin, non-responsive, or was unable to find the call. The information presented only includes the tracebacks where you identified the listed providers; the providers may also have appeared in these positions for other tracebacks as well.

Provider	Total Hops	Open	POE	Orig	No Resp	Not Found
Telconus / Telcon US / Telcon Voice / Whisl	9	0	0	0	0	0

If you have any trouble seeing this email, please visit:
<https://portal.tracebacks.org/providers/provider/summaries/386>

*This email was sent from a notification-only address that does not accept incoming email. Please do not reply to this message - send inquiries to **support@tracebacks.org***

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 14 Nov 22 22:34 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:
<https://portal.tracebacks.org/hops/hop/61007>
(URL is a private login; do not share.)

Call Details for Traceback #11232 0 seconds ago

Campaign:	Amazon-SuspiciousCharge-P1
Date/Time:	2022-11-10 20:03:03 +0000 UTC
To:	+13029301007
From:	+13156423312
Calls to wireless numbers impersonating Amazon, claiming suspicious activity on customer's account	

*This email was sent from a notification-only address that does not accept incoming email. Please do not reply to this message - send inquiries to **support@tracebacks.org***

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 16 Nov 22 13:50 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

<https://portal.tracebacks.org/hops/hop/61177>

(URL is a private login; do not share.)

Call Details for Traceback #11281 0 seconds ago

Campaign: StudentLoan-ProcessingCenter
Date/Time: 2022-11-15 18:35:15 +0000 UTC
To: +19737807866
From: +16823530811

Calls to recipients from the processing center regarding big changes to the student loan program. Recipients may not have student loans. Evidence suggesting lack of consent, including consumer complaints, honeypot data, and other information. Note FCC 11/4/22 Enforcement Advisory reminded providers to aggressively police unlawful robocalls regarding student loans. According to the Advisory: "These calls typically state that the caller is informing the recipient that the payment suspension will end or that a petition can be filed on their behalf to get a certain amount of their loan 'dismissed.' Some common campaigns purport to be from the 'student loan forgiveness center' or from a state forgiveness center."

This email was sent from a notification-only address that does not accept incoming email. Please do not reply to this message - send inquiries to support@tracebacks.org

From: traceback-notice@tracebacks.org
To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com
Date: 01 Dec 22 09:30 UTC

INDUSTRY TRACEBACK GROUP

Monthly Metrics - **Smartbiz Telecom, LLC**

[Redacted], you can find your organization's traceback-related metrics for the last 30 days below.

Your Summary:

Total Hops	Open	POE	Downstream	Orig	No Resp	Not Found	Avg Response	Campaigns
2	0	0	0	0	0	0	32 minutes 36 seconds	2

Upstream Summary:

This table shows the providers who you have identified as an upstream provider in response to tracebacks. The chart displays the number of occurrences in which each of those providers is the Point of Entry, Origin, non-responsive, or was unable to find the call. The information presented only includes the tracebacks where you identified the listed providers; the providers may also have appeared in these positions for other tracebacks as well.

Provider	Total Hops	Open	POE	Orig	No Resp	Not Found
Telconus / Telcon US / Telcon Voice / Whisl	3	0	0	0	0	0

If you have any trouble seeing this email, please visit:
<https://portal.tracebacks.org/providers/provider/summaries/386>

*This email was sent from a notification-only address that does not accept incoming email. Please do not reply to this message - send inquiries to **support@tracebacks.org***

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 09 Dec 22 17:41 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:
<https://portal.tracebacks.org/hops/hop/62742>
(URL is a private login; do not share.)

Call Details for Traceback #11540 0 seconds ago

Campaign: Amazon-AuthorizeOrder

Date/Time: 2022-12-07 14:45:01 +0000 UTC

To: +15127794885

From: +15129550991

Calls to wireless numbers impersonating Amazon, calling to authorize an order that was placed.

*This email was sent from a notification-only address that does not accept incoming email. Please do not reply to this message - send inquiries to **support@tracebacks.org***

From: traceback-notice@tracebacks.org
To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com
Date: 14 Dec 22 14:01 UTC

INDUSTRY TRACEBACK GROUP

We are notifying you that **Smart Network Solutions Communications Corp** has not yet responded to the request for Traceback #11540.

We encourage you to follow up with **Smart Network Solutions Communications Corp** to participate in the traceback process.

We can not change results after the traceback has closed.

Please note that FCC regulations require voice service providers to respond fully and in a timely matter to all traceback requests from the Industry Traceback Group, as the designated traceback consortium.

If your upstream provider **Smart Network Solutions Communications Corp** is having trouble accessing the portal please have them contact **support@tracebacks.org**

Review the traceback via our secure on-line portal:
<https://portal.tracebacks.org/hops/hop/62742>
(URL is a private login; do not share.)

*This email was sent from a notification-only address that does not accept incoming email. Please do not reply to this message - send inquiries to **support@tracebacks.org***

From: traceback-notice@tracebacks.org
To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com
Date: 01 Jan 23 09:30 UTC

INDUSTRY TRACEBACK GROUP

Monthly Metrics - **Smartbiz Telecom, LLC**

[Redacted], you can find your organization's traceback-related metrics for the last 30 days below.

Your Summary:

Total Hops	Open	POE	Downstream	Orig	No Resp	Not Found	Avg Response	Campaigns
1	0	0	0	0	0	0	52 minutes 44 seconds	1

Upstream Summary:

This table shows the providers who you have identified as an upstream provider in response to tracebacks. The chart displays the number of occurrences in which each of those providers is the Point of Entry, Origin, non-responsive, or was unable to find the call. The information presented only includes the tracebacks where you identified the listed providers; the providers may also have appeared in these positions for other tracebacks as well.

Provider	Total Hops	Open	POE	Orig	No Resp	Not Found
Smart Network Solutions Communications Corp	1	0	1	0	0	0

If you have any trouble seeing this email, please visit:
<https://portal2.tracebacks.org/providers/provider/summaries/386>

*This email was sent from a notification-only address that does not accept incoming email. Please do not reply to this message - send inquiries to **support@tracebacks.org***

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 25 Jan 23 20:47 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

<https://portal.tracebacks.org/hops/hop/65421>

(URL is a private login; do not share.)

Call Details for Traceback #11970 0 seconds ago

Campaign: Employee-RefundCredits

Date/Time: 2023-01-24 20:48:39 +0000 UTC

To: +12532799944

From: +12186071382

Prerecorded calls suggesting availability of employee refund credit. Caller does not appear to identify the entity responsible for the call, as identified entity does not appear to have any online presence. Prerecorded calls made to wireless numbers as well to numbers on the National Do Not Call Registry apparently without consent or prior relationship. Evidence of high-volume calling and consumer complaints about campaign.

This email was sent from a notification-only address that does not accept incoming email. Please do not reply to this message - send inquiries to support@tracebacks.org

From: traceback-notice@tracebacks.org
To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com
Date: 01 Feb 23 09:30 UTC

INDUSTRY TRACEBACK GROUP

Monthly Metrics - Smartbiz Telecom, LLC

[Redacted], you can find your organization's traceback-related metrics for the last 30 days below.

Your Summary:

Total Hops	Open	POE	Downstream	Orig	No Resp	Not Found	Avg Response	Campaigns
1	0	0	0	0	0	0	35 minutes 48 seconds	1

Upstream Summary:

This table shows the providers who you have identified as an upstream provider in response to tracebacks. The chart displays the number of occurrences in which each of those providers is the Point of Entry, Origin, non-responsive, or was unable to find the call. The information presented only includes the tracebacks where you identified the listed providers; the providers may also have appeared in these positions for other tracebacks as well.

Provider	Total Hops	Open	POE	Orig	No Resp	Not Found
Telconus / Telcon US / Telcon Voice / Whisl	1	0	0	0	0	0

If you have any trouble seeing this email, please visit:
<https://portal.tracebacks.org/providers/provider/summaries/386>

This email was sent from a notification-only address that does not accept incoming email. Please do not reply to this message - send inquiries to support@tracebacks.org

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 01 Feb 23 20:17 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:
<https://portal.tracebacks.org/hops/hop/65924>
(URL is a private login; do not share.)

Call Details for Traceback #12078 0 seconds ago

Campaign: Utility-30MinDisconnect

Date/Time: 2023-01-30 15:21:13 +0000 UTC

To: +19177332656

From: +19174236602

Recorded message says your electric service will be disconnected in 30 to 45 minutes. Utility company is not always identified. Assorted toll-free or other numbers used as caller-ID.

This email was sent from a notification-only address that does not accept incoming email. Please do not reply to this message - send inquiries to support@tracebacks.org

From: traceback-notice@tracebacks.org

To: noc@smartbiztel.com, katherine.rosales@smartbiztel.com, eborrero@smartbiztel.com

Date: 02 Feb 23 14:25 UTC

INDUSTRY TRACEBACK GROUP

To Whom It May Concern:

As part of a traceback conducted by the Industry Traceback Group, your network has been identified in the call path for voice traffic that has been deemed suspicious and potentially illegal.

U.S. Federal Communications Commission regulations may legally require your cooperation with this request. Therefore, the Industry Traceback Group requests that you respond to this traceback inquiry as soon as possible, but no later than three business days from now, to assist in identifying the source of this suspected fraudulent, abusive or unlawful network traffic.

More information about the Industry Traceback Group and the traceback process is available at <https://tracebacks.org/the-industry-traffic-group-itg-for-providers/>.

Responding to This Request

Your response to this inquiry should be submitted via the Industry Traceback Group's secure online portal. The online portal includes information on any traceback request involving your network, including call detail information of suspicious traffic. **For confidentiality and security purposes, provide this information only through the online portal. Do not provide the information via email.**

1. The source of the traffic and the identity of the upstream voice service provider(s) that sent the traffic into your network. If one of your end users originated the traffic, the identity of that end user.
2. If, in investigating the traffic, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations in the portal's comments section.
3. Any actions and mitigation steps you have taken on your network to ensure compliance with applicable U.S. laws and regulations and to prevent the suspected illegal traffic from continuing to reach U.S. subscribers.

The Industry Traceback Group believes that every voice service provider has a responsibility to help stop illegal robocalls. Therefore, to the extent that this traceback identifies the originator of these suspicious robocalls, the Industry Traceback Group urges that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, the ITG may (1) provide information to downstream voice service providers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process; and/or (2) advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so.

Please feel free to consult with your counsel on this request.

For help or questions, email support@tracebacks.org.

Submit your response via our secure on-line portal:

<https://portal.tracebacks.org/hops/hop/65957>

(URL is a private login; do not share.)

Call Details for Traceback #12079 0 seconds ago

Campaign: Utility-30MinDisconnect

Date/Time: 2023-01-30 15:50:33 +0000 UTC

To: +16237766263

From: +16239994024

Recorded message says your electric service will be disconnected in 30 to 45 minutes. Utility company is not always identified. Assorted toll-free or other numbers used as caller-ID.

This email was sent from a notification-only address that does not accept incoming email. Please do not reply to this message - send inquiries to support@tracebacks.org